LA-SUB--93-306

Topical Report No. SEASF-TR-90-009
November 1990

Evaluation of Safety Assessment Methodologies in Rocky Flats Risk Assessment Guide (1985) and Building 707 Final Safety Analysis Report (1987)

by

Bob Walsh, Colin Fisher, and Gilbert Zigler
Science and Engineering Associates, Inc.
SEA Plaza
6100 Uptown Boulevard, NE
Albuquerque, NM 87110

DISCLAIMER

Science & Engineering Associates, Inc.

Evaluation of Safety Assessment Methodologies

in

Rocky Flats Risk Assessment Guide (1985)

and

Building 707 Final Safety Analysis Report (1987)

by

Bob Walsh, Colin Fisher, and Gilbert Zigler

Science and Engineering Associates, Inc.

Topical Report No. SEASF-TR-90-009

November 1990

Science &
Engineering
Associates, Inc.
SEA Plaza
6100 Uptown Blvd. NE
Albuquerque, New Mexico 87110
(505) 884-2300

November 9, 1990

Mr. Leon Borduin
N-6 Division, MS K557
Los Alamos National Laboratory
Los Alamos, NM 87545

Subject: Transmittal of Report "Evaluation of Safety Assessment Methodologies in Rocky Flats Risk Assessment Guide (1985) and Building 707 Final Safety Analysis Report (1987)"

Reference: Subcontract 9-X50-8194N-1, Task Order 005

Dear Mr. Borduin:

Enclosed please find SEA Topical Report SEASF-TR-90-009 entitled "Evaluation of Safety Assessment Methodologies in Rocky Flats Risk Assessment Guide (1985) and Building 707 Final Safety Analysis Report (1987)." We appreciate your review of the draft report and the comments and suggestions you provided. This report incorporates your comments and suggestions.

Four bound copies of the SEA report are enclosed for your use. Please call if you have any questions or if you need our assistance.

Sincerely,

SCIENCE AND ENGINEERING ASSOCIATES INC.

Robert A. Clark
Principal Investigator

RAC:blm

cc (wo/encl): A. Neuls, N-6
cc (w/encl): C. Warner, N-6
C. Fisher, SEA
R. Walsh, SEA
G. Zigler, SEA

Evaluation of Safety Assessment Methodologies in Rocky Flats Risk Assessment Guide (1985) and Building 707 Final Safety Analysis Report (1987)

Table of Contents

Evaluation of Safety Assessment Methodologies in Rocky Flats Risk Assessment Guide (1985) and Building 707 Final Safety Analysis Report (1987)

1. INTRODUCTION

1.1 Background

FSARs. Rockwell International, as operating contractor at the Rocky Flats plant, conducted a safety analysis program during the 1980s. That effort resulted in Final Safety Analysis Reports (FSARs) for several buildings, one of them being the *Building 707 Final Safety Analysis Report, June 87* (707FSAR) and a Plant Safety Analysis Report. *Rocky Flats Risk Assessment Guide, March 1985* (RFRAG85) documents the methodologies that were used for those FSARs.[1]

Resources available for preparation of those Rocky Flats FSARs were very limited. After addressing the more pressing safety issues, some of which are described below, the present contractor (EG&G) intends to conduct a program of upgrading the FSARs. This report presents the results of a review of the methodologies described in RFRAG85 and 707FSAR and contains suggestions that might be incorporated into the methodology for the FSAR upgrade effort.

Systematic Evaluation Program. As a result of the Defense Nuclear Facilities Safety Board (DNFSB) recommendation for long-term safety improvements, the DOE has decided to develop and implement a Systematic Evaluation Program (SEP) at the Rocky Flats plant over about the next four years.[2-5] The purpose of this program will be to assure proper evaluation and coordination of the facility changes under consideration. With respect to the SEP, the DNFSB recommended that the DOE:

- Take a balanced approach concerning the criteria for improving the seismic resistance of safety equipment and the criteria for improving seismic resistance of the building housing such equipment;
- Consider other external events and related design improvements in an integrated manner to ensure a balanced and integrated level of safety;
- Consider in the same integrated fashion the safety issues regarding a comparison of existing facility design features with those required by commercial criteria and standards, such as fire protection, as well as the impact of expected new criteria and standards, such as life extension;
- Place appropriate emphasis on improving defense in depth as a means for enhancing safety at the plant;
- Consider using probabilistic results, to the extent reasonable, in assisting in the integration process;
- Conduct the review with a process that is flexible to accommodate the levels of protection to public health and safety appropriate to the differing operations carried out in the various buildings at Rocky Flats;

- Take full account of the methodology and experience developed by the commercial power reactor industry for dealing with similar issues; and

- Establish a backfit policy applicable to the Rocky Flats plant to provide a framework for making decisions on which facility changes identified under the SEP will or will not be implemented.

The DNFSB further recommended that the Rocky Flats SEP address all outstanding current safety issues and include, but not be limited to, consideration of the following items:

- Effects of severe external events, with particular emphasis on seismic events and high winds;

- Effects of severe internal events with particular emphasis on fire;

- Ventilation system performance under severe external and internal events, including redundancy consideration;

- Interaction of equipment and structures due to severe internal and external events; and

- The basis and procedures for making backfit decision on which the facility changes identified under the new program will or will not be implemented.

1.2 Purpose of This Report

Science and Engineering Associates, Inc. (SEA) was requested by the Los Alamos National Laboratory (Los Alamos) to review the methodologies used in RFRAG85 and 707FSAR. This effort was performed in the months of June through September 1990 for a total level of effort of approximately 8 staff months. A trip to Rocky Flats including a detailed familiarization tour of Rocky Flats Building 707 was also undertaken by the principal SEA contributors as part of the review effort.

The objectives of this review were to provide Los Alamos with independent insights into the following topics:

- Review and provide comments on the methodology delineated in the RFRAG85 and 707FSAR,

- Evaluate the applicability and limitations of the methodology with respect to the facilities and types of operations conducted at the Rocky Flats plant, and

- Provide recommendations for potential enhancements to the methodology.

1.3 Acknowledgements

This document incorporates extensive comments contributed by Stan Logan of S.E. Logan and Associates. Mr. Bob Clark, the SEA program director, provided guidance and expert review of this document. Messrs. Bob Knudson and Steve Ross, also of SEA, provided considerable support by assisting with the acquisition of background reports and general information of Rocky Flats.

2. GENERAL OBSERVATIONS

2.1 Purpose of Risk Assessment

The methodology used in a risk assessment is determined in part by the required format and content of the final report. The format and content may be specified by the sponsoring agency, but they must reflect the primary objectives of the risk analysis. For the Rocky Flats plant, we suggest that the objectives of the risk analyses are:

- To bound the risks from the Rocky Flats plant as tightly as is reasonably achievable;
- To compare the maximum risks from the Rocky Flats plant to actual risks from other hazards of the same character;
- To communicate those comparisons as clearly as possible to the DOE, to its advisory boards, and to the public; and
- To document the process of each risk analysis in sufficient detail that a knowledgeable person can audit the process by hand without reference to other documents.

DOE Orders require that the risk assessment

- Assess facilities as they exist or are likely to be built, not as they were conceived;
- Assess human reliability that would be expected with current management, not with perfect operation; and
- Be scoped to cover classes of operations so that individual operations are bounded by a risk that is acceptable to the DOE, rather than scoped to analyze individual operations to obtain a best estimate of total risk.[6-7]

However, to assure a balanced approach in the SEP, the methodology must also identify the classes of operations and hazards whose risk bounds are the dominant contributors to the total risk bound.

2.2 Bounding Risk Curves

Total Expected Risk. Section 8.4 of RFRAG85 refers to the safety analysis process as though its objective were to "estimate the total expected risk of a facility." A lesser goal, to determine an upper bound on the total expected risk of a facility, is all that is required and the most that should be claimed.

Figure 2-1 shows a family of risk curves. The figure is taken from Figure 7.1-1 of RFRAG85. The curve for p=0.75 shows a frequency of about 10^{-4} per year for a consequence of about 10 man-rem. If this were presented in a FSAR, it should be made clear that the 75th percentile was arrived at conservatively. That is, there is at least a 75% probability that accidents more severe than 10 man-rem will occur less often than 10^{-4} per year.

Bounding the Uncertainty. However, the family of risk curves in Figure 2-1 would not be very encouraging. They say nothing about the remaining 25 percentiles. The mean frequency over the rest of the probability distribution may be much higher. If the exposure time for the risk is forty years, then there are two cases to consider:

- Seventy-five percent of such consequences would have a frequency less than 10^{-4} per year for such accidents.
- Twenty-five percent of such consequences would have a frequency greater than 10^{-4} per year, perhaps as much as one per year, one thousand per year, or one million per year.

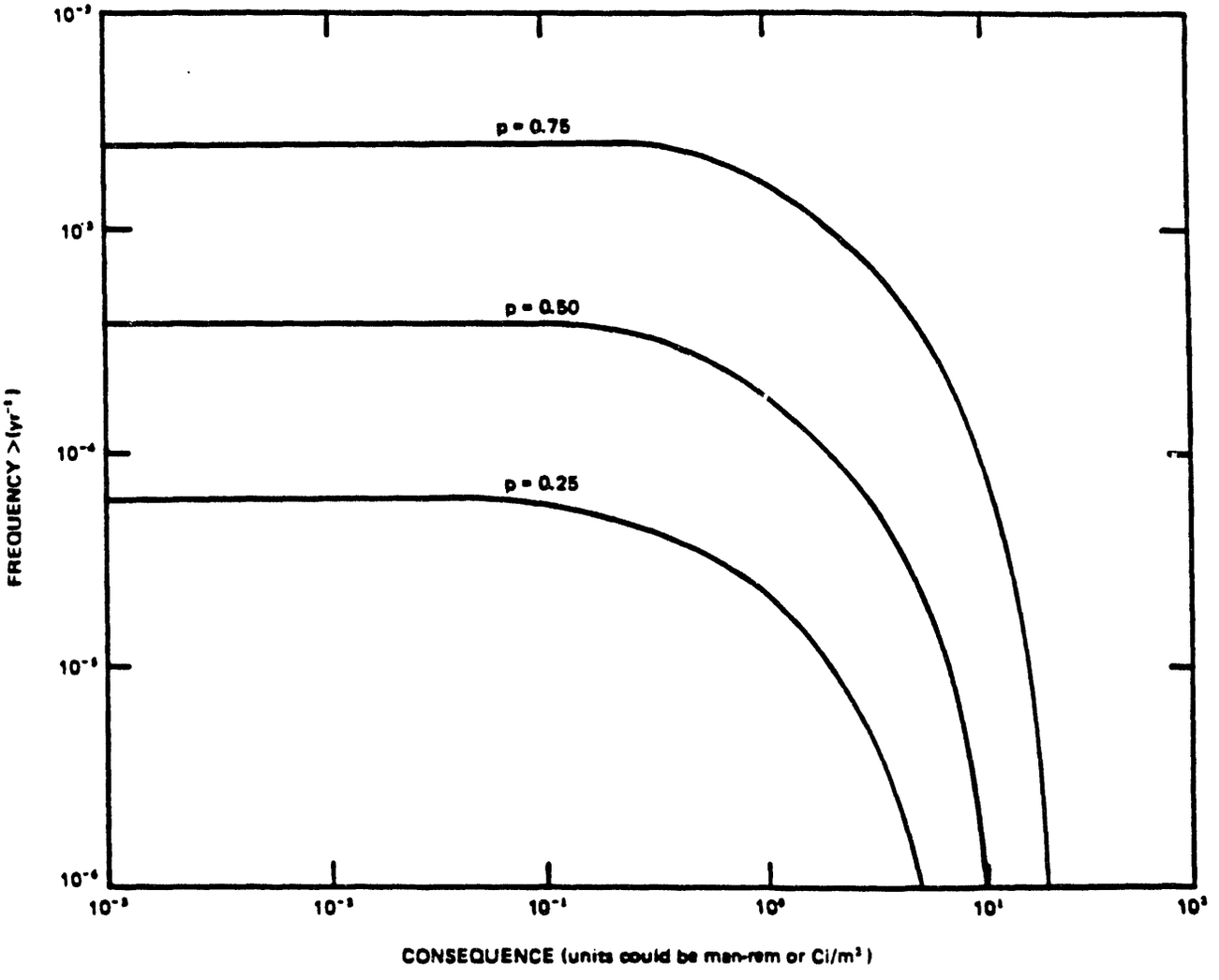

Figure 2-1. RFRAG85 Figure 7.1-1

The most we can conclude from this information is that the probability of such an accident occurring in forty years is less than 0.253, which is the value of

$$0.25 + 0.75\,(1 - e^{-.004}).$$

The discussion of Section 8.2.5 of RFRAG85 characterizes the 90th percentile risk curve as a "conservative estimate." But there is a 10% probability that the risk is greater than the 90th percentile. Without further information that characterizes the tail of the distribution, it is not possible to conclude that the risk of a severe accident is acceptable. A FSAR would have to indicate the 99.99th, 99.999th, and 99.9999th percentile or indicate how they may be inferred.

We suggest that a family of risk curves is not only inadequate to describe the risk of severe consequences, but is also unnecessarily confusing for a final risk presentation in a FSAR. The family of risk curves could be replaced by two simpler graphs. One would be an upper bound conservative probability distribution for the total frequency of all accidents with non-zero consequence, such as in Figure 2-2. This would represent the asymptotic behavior of the risk curves at low consequence.

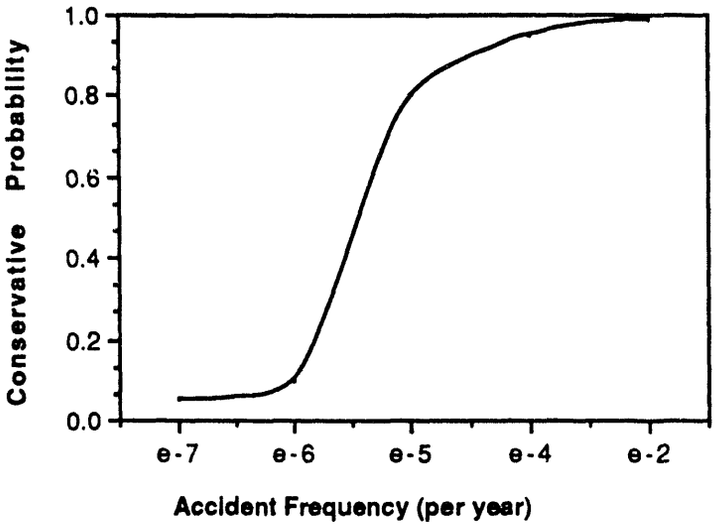

Figure 2-2: Conservative Cumulative Probability Distribution

The other graph would contain a maximum-probability curve over the range of severe consequences. The ordinate would be probability of an occurrence during the life of the plant. For each consequence, the curve would show an upper bound on the expected probability of occurrence, as in Figure 2-3. That is, it would be an upper bound on the result that would be obtained if:

- Each risk curve were converted from frequency to failure probability, using the expected facility life, and
- The expected failure probability for each consequence was obtained by integrating over the risk curves.

This approach presents the results of integration over all risk curves at a given consequence; i.e., the expected value of the conservative analysis which is called a "maximum."

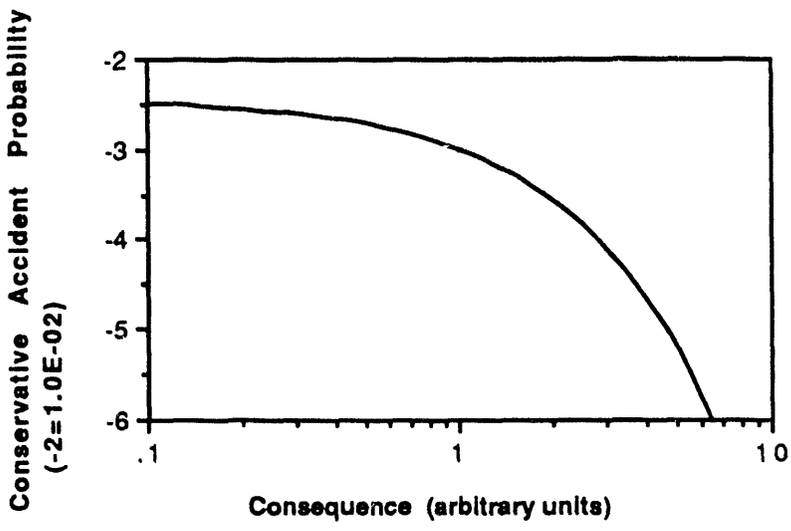

Figure 2-3: Maximum Probability Distribution

Presentation of Major Accident Categories. RFRAG85 correctly requires separate reporting of frequency and consequence for major categories of accidents. It would be useful if RFRAG85 also required reporting the estimated consequences of accidents investigated but found to have an estimated frequency less than one per million years.

The 707FSAR, Page 2-5, states that the report looks at realistic estimates of the consequences of severe accident scenarios and the impact of uncertainty on those estimates. Ranges of values are said to be used throughout the analysis wherever possible and realistic values, together with ranges of uncertainty, are used in the final result. The summary Table 2.2-1 of 707FSAR offers no such indication of the ranges of uncertainty in the results. The radiological doses are compared to DOE guidelines (Order 5480 series). In the NRC world, comparisons of calculated radiological doses for siting evaluations to the guidelines of 10 CFR Part 100 are made for conservatively calculated doses. There can easily be several orders of magnitude between realistically calculated and conservatively calculated radiological doses. Therefore, the approach taken in the 707FSAR is potentially nonconservative by several orders of magnitude. Figure 2.3-3 of 707FSAR does show the uncertainty in the summary results in graphical form. This presentation would be improved if the estimated uncertainty associated with each event analyzed was shown in the table (such as 707FSAR Figure 2.3-4) so the relative contributions to the overall uncertainty could be assessed.

2.3 Comparison with Other Risks

Any comparison of the maximum risk from a Rocky Flats facility to accepted actual risks from other hazards should be consistent with current understanding of how public perceptions of risk are guided by the character of the hazard. Social psychologists have found that:

- Familiar hazards are more acceptable than unfamiliar ones;
- Voluntary risks tend to be accepted readily; whereas involuntary risks are resisted;

- Risk is more acceptable where an individual has some control than where one's life is entirely in someone else's hands;
- Risks are judged in relation to their perceived benefits; and
- One of the most influential characteristics of a hazard is the potential it poses for catastrophe, for killing hundreds or thousands of people at once.[8]

Occupational risk is voluntary and has an immediately perceived benefit. The hazards are or should become familiar. Many hazards at Rocky Flats are under the control of the worker most likely to be injured. Therefore, we suggest that a FSAR compare the occupational risks with those in other occupations.

For the public, on the other hand, exposure to toxic materials from Rocky Flats is an unfamiliar hazard and the hazard is out of the individual's control. To the extent that the hazard may be transported beyond the immediate neighborhood of Rocky Flats, such as by animals, plants, weather, or drainage, it is involuntary. In addition, the perceived benefit may be altered by the changing geopolitical situation. Therefore we suggest that a FSAR compare the risks of severe Rocky Flats accidents with risks of severe accidents from other hazards that are unfamiliar, uncontrollable, and/or involuntary.

2.4 Documentation of the Process

Probability of Frequency. Section 7.1 of RFP-AG85 adopts a subjective definition of probability. Martz and Waller point out that "... the subjective probabilities assigned to a particular hypothesis by one individual may be quite different from those that would be assigned by some other individual."[9] Reliance on a subjective definition opens a risk analysis to the criticism that its risk bounds are not reproducible. Therefore, the argument might proceed, the calculated risk bound may not represent the risk bound that would be determined by other knowledgeable individuals, such as officials of the DOE, members of a DOE advisory board, or experts representing the interests of the general public.

We suggest that any definition of probability that is presented in a FSAR, whether directly or by reference, be based on objective concepts. Appendix C presents one possible approach to establishing an objective definition of probability of frequency.

References. A FSAR is a document that should be as self-contained as possible, with a minimum of references. Where references are used, they should have complete citations and be readily available. We suggest that methodology references be cited in a methodology report, separate from the risk assessment guide. For software, for instance, the methodology report should include configuration identification, detailed descriptions of the encoded models and data, summaries of software test results, and any other information that bears on software reliability. The methodology report should also describe the quality assurance procedures that are applied to the risk analysis process.

3. OVERALL APPROACH

Scope. RFRAG85 emphasizes calculation of risk of accidental plutonium releases, stating that the same techniques address other radioactive materials and toxic chemicals. We suggest that all of these hazards be considered simultaneously. It is more efficient to consider all consequences in a failure mode effects analysis, for instance, than to perform a separate analysis for each type of consequence.

The emphasized operations are chemical processing, metal working, research and development, and waste processing. Risk assessment is also needed for modification, special maintenance, deactivation, decontamination, and decommissioning. This should not require any additional methodologies, because a methodology that is applicable to the diverse normal processes of the Rocky Flats plant should be adequate for these special activities.

Safety Document Control. We recommend that the risk assessment methodology include a document control system. A document control procedure should state which documents are subject to configuration control and should either describe a separate Configuration Management System for plant safety documents or else specify an interface with a more general Configuration Management System. The system should control not only Safety Analysis Reports, but nearly all records of safety engineering, including safety notebooks, risk analysis software configurations and test results, and minutes of review meetings. Each risk assessment should identify the specific plant configuration being evaluated, using specific reference to a configuration management system for facility design documents.

Safety Quality Assurance. In order to limit the probability of human error or software error in the risk assessment process, we recommend that the process be subject to strict quality control. We suggest that formal quality assurance procedures and guidelines be developed for safety engineering, implementing at least the DOE quality assurance requirements.[10]

4. ACCIDENT FREQUENCY ANALYSIS METHODOLOGY

4.1 Hazard Identification Methodology

Completeness. The most severe error in a risk assessment is omission of a severe hazard. One way to assure complete coverage of hazards is to scrutinize the design more than once, using different formal procedures. We suggest that each facility be surveyed for hazards by every reasonably applicable methodology. Appendix A contains suggested procedures and/or details for several formal hazard analysis methods.

RFRAG85 specifies Preliminary Hazard Analysis (PHA) and Failure Mode and Effects Analysis (FMEA), both of which are appropriate tools for locating potential hazards. If either of these steps were omitted, there would be much less confidence that all potential accidents had been identified.

For the batch chemical processes being performed at Rocky Flats, we suggest that the PHA and FMEA be preceded by analyses that clarify the functional relationships among process stages. Two such tools are HAZOPS and the digraph method, which can also be used to model control systems.

The FMEA may miss some potential initiators that involve multiple failures. The FMEA should be followed by development of Initiating Events Logic Diagrams (IELDs). An IELD is a top-down analysis for a particular class of accident initiator.

Appendix A suggests guidelines for all of the procedures mentioned above.

External Hazards. RFRAG85 provides good coverage of natural phenomena. We suggest that the coverage be extended to include consequences from adjacent facility accidents and building damage by vehicular accidents.

We suggest that a methodology be developed for assessment of on-site transportation accidents, for use in the site safety analysis report.

Initiating Event Categories. The initiating events should be gathered into categories to simplify the tabulation of safety system response. All initiating events in a category should have the same or equivalent local effects. This conforms to the requirement that the safety analysis be "scoped wherever possible to cover classes of ... operations within a facility ... so that individual operations ... are bounded by the general analysis."[6] (If IELDs have been prepared, a category may correspond to one IELD or one major branch.)

4.2 Design Basis Analysis Methodology

Defense in Depth. The DOE requires that nuclear facilities be designed conservatively. Some of the principles of conservative design are:

- Wide margins for error, such as temperature design requirements that are above any expected temperature;
- Redundancy;
- Emergency safety systems;

- Nested confinement/containment volumes; and
- Remote siting.

Definition of Failure and Success Criteria. For both qualitative and quantitative analysis, it is important to have a consistent definition of failure and success criteria. We suggest that the terms "failure" and "rating" be defined such that they are correlated. That is, if a component is subjected to loads that are within its ratings, but does not or is not able to perform its intended function, then that is a failure. If any load exceeds its rating, the component is not expected to perform its function, but the absence of function under those circumstances is not considered a failure of the component.

Components are typically derated; that is, the rated load for a particular component failure mode would be much more than the expected load on the system. The mode failure rate may be modeled with a dependence on the extent of derating, usually expressed as a dependence on the stress ratio, the ratio of actual load to rated load. To be conservative, a model of failure rate dependence on stress ratio will only be used for stress ratios less than one. Whenever the load on a component exceeds the rating for a failure mode, such as when damage is propagated, a conservative analysis assumes that the component fails in that mode.

Design Basis Accidents. The DOE defines Design Basis Accidents as accidents "for which the confinement structure, systems, components, and equipment must meet their functional goals."[11] In the context of probabilistic risk analysis, the ratings of these items must be such that all expected stress ratios from design basis accidents will be less than one. The actual ratings may be higher than required to meet a given design basis requirement, either because of deliberate provision of a safety factor or because the higher rating is required to meet another requirement.

As knowledge increases, the design bases for new facilities may change. One must be careful not to confuse new design bases with original design bases. We suggest that the FSAR for a particular building use the term "design basis" to refer to the logic that underlies decisions made in that particular building design. New knowledge may change estimates of accident frequencies or accident consequences, and it may change the requirements for continuing to operate or for modifying an existing building, but it does not change the design basis for something that has already been designed.

Top-Down Facility Analysis. The RFRAG85 methodology for plant familiarization is basically bottom-up, from initiator to consequence. Top-down analyses are performed only for individual systems. This is a beginning, but hazard identification should be followed by top-level, top-down facility analyses to assure that all potential accidents are identified, whether or not they have well-defined initiators.

We suggest that a top-down analysis be prepared that completely documents the safety design basis, including redundancy and defense-in-depth. This analysis might consist of success trees for the containment of releases, the safe evacuation of workers, the preservation of the environment, and the control of damage to the facility.

We further suggest that all of the design basis analysis be supported by deterministic calculations. These would show, given certain failures, what loads would be placed on other components. Such calculations are part of the risk assessment; they should be subjected to full quality assurance procedures.

The blind use of reactor PRA methodologies on facilities such as Rocky Flats is fraught with potential problems. Top-level analysis of commercial reactor designs is not usually presented, but it is implicit in the establishment of Level I, II, and III Probabilistic Risk Analyses. The implied top-down analysis branches once on the integrity of the containment and a second time on the integrity of the

reactor core. This structured breakdown, however, is not directly applicable for the Rocky Flats plant since there are no clear-cut boundaries as in the commercial reactors: fuel element case - reactor vessel - containment building.

Accident Initiation. Without a top-level top-down analysis, it is difficult to assure that there are no combinations of normal operations, typically rare in occurrence, that can lead to partial or complete facility failure without any component failure or operator error; that is, without an initiator. For instance, normal operation may cause a buildup in contamination at some point within containment, followed by release of that buildup during a rare maintenance procedure. Another example would be an unusual combination of breaker settings which could cause a loss of power to an instrument which in turn would cause the defeat of an accident mitigation system.

The methodology presented in RFRAG85 assumes that all operational accidents have an identifiable initiator. This may be true; it may not be necessary to include any additional methodologies. However, the matter should be left open until hazard identification and design basis analysis are completed and all of the identified accidents have been shown to result from an initiating event.

4.3 Accident Sequence Development Methodology

Safety System Response. Potential mitigating actions in response to an accident initiator include both operation of engineered safety systems and intervention by operators. These responses are modeled in event trees, as discussed in Section 2.2 of RFRAG85.

Support Systems. Section 2.2.2 of RFRAG85 is correct in requiring that support system responses appear in the event tree if they may affect two or more safety systems. The analyst should consider the potential effect of a support system on all safety systems, because its failure may inadvertently impact safety systems other than those it was designed to support.

In the 707FSAR, Page 8-9, a model for fire suppression is described that is not justified and seems out of place in the context of a frequency-based risk analysis. Following this model in the text is a model for leakpath factors, given a fire, that is also not well-justified.

System Failure Effects. Although a system normally has only one success state, it may have multiple failure states. If the accident consequences or the subsequent system operations may differ for different failure states, then the tree should separate into three or more branches at that point.

System Dependencies. Section 2.2.2 of RFRAG85 assumes that all dependencies at system level are deterministic, whereas in actual situations they may often be probabilistic. That is, the fault tree for one system may contain basic events or conditional states whose probability depends on the operation or failure of another system. This may cause the split fraction to depend on the accident sequence.

For a bounding analysis, the risk assessment can and should use worst case split fractions wherever possible. To make this feasible, it is necessary to construct the event tree such that system failure always increases the risk. Therefore, in the event that success of a system is undesirable in a particular accident sequence, the event tree should assume that the function is always successful. For example, if a fire causes a HEPA filter to fail open (loss of filtration), no credit should be taken for mitigation by failure of a blower in the system.

Page 8-10 of the 707FSAR discusses a fire in a glovebox owing to a loss of inert atmosphere where combustible material (Pu) is present only 1% of the time. However, all of the gloveboxes and conveyors associated with modules A, B, and C have a common inert ventilation system so the 1% figure

would be expected to be close to 100%. Another example of no consideration for propagation considerations can be found in Page 8-55 of the 707FSAR where it discusses damage to a glovebox by a wooden plank driven by a tornado through the building exterior wall. It goes on to say that the ventilation continues to operate with benign radiological consequences. The analysis is deficient in that damage to other ventilation system components were not analyzed, particularly major ducts or ventilation system components on the second floor.

The multitude of potential fire scenarios are very critical for Building 707, some of which apparently were not considered in detail or the results of these considerations were not documented. Page 8-11 of the 707FSAR states that damage owing to a glovebox fire would be limited to the glovebox itself and contamination of the room for credible accident scenarios. This does not address the effects of the lack of exhaust HEPA filters on some gloveboxes and the loss of production resulting from dispersal of plutonium combustion products throughout the exhaust ventilation plenum up to and including the second floor filtration components and ducting. Page 8-11 also addresses fire outside a glovebox and states a mitigating feature is that combustible material in a module will be present only 1% of the time. Since the plant has been shut down for 9 months, and the aisles of many of the modules had lots of combustible material during our recent inspection, following resumption the module would have to have no combustible material present for 900 months to retain the validity of the estimate. In other words, the 1% sounds very low.

Adverse Functions. Any safety system that might be activated in response to an initiator should be checked not only for mitigating functions, but also for potential adverse functions or failures. Attempted recovery actions may have an adverse effect. These potential operator errors should be included in the analysis. As an example, Page 8-11 of the 707FSAR discusses worker risk for a glovebox fire and assumes a respirator can be donned within 15 seconds and the area evacuated within 2 minutes, the worker dose does not exceed DOE guidelines. There is no discussion of the probabilities that these actions can be successfully accomplished or discussion of the consequences should they be unsuccessful.

Simplification. For a bounding analysis, safety systems which are not specifically designed to prevent or mitigate the consequences of the class of initiating events should be omitted from the list of responders. Because of the inherent uncertainties in the frequencies and consequences of the initiators, we suggest that RFRAG85 be extended to provide guidelines for the minimum effectiveness required of a mitigating safety system function for its inclusion as a potential responder to a class of initiators. The guidelines should specify a minimum design frequency of prevention or mitigation and a minimum design effect on consequences. However, an adverse safety system function should be included at this stage regardless of its design frequency.

Documentation Errors. Section 2.2.2 of RFRAG85 contains some errors, which appear to be typographical or editorial, that happen to affect the definition of the methodology. These are:

- The numbered steps refer to safety systems, but are clearly intended to apply to all systems that appear in the event tree, including support systems.

- Step (4), paragraph 2, line 9 should be: "function, and (3) the operation of the system" instead of: "function, or (3) the operation of the system".

- Step (5) is confusing in that it implies that sequences are quantified in this step, whereas that it clearly not the case. The description also refers to "conditional probabilities" for each branch of the event tree in Figure 2.2-2. In fact, however, there is no discussion anywhere else of calculating conditional probabilities, and the figure implies that the fault tree and therefore the probability for F2 are not conditional on the accident sequence. As noted above, only worst-case split fractions are all that are needed for a bounding analysis. Therefore, the discussion of frequency

of accident sequence occurrence should be moved to Section 2.5.3, and the term "conditional probabilities" should be clarified or eliminated.

Externally-Initiated Accidents. RFRAG85 provides no procedure for analyzing events following an external initiator. The methodologies described do not appear to be capable of quantifying event trees that have strongly correlated split fractions.

We suggest that accident sequences be developed for all initiators, especially natural phenomena that reach "incipient failure" levels. The effects of split fraction dependency can be bounded. Furthermore, there are now analysis tools, such as RISKMAN, that can treat split fraction dependency if that is desired.

4.4 Availability Analysis Methodology for Safety Systems

System Availability Data. Section 2.3.2 of RFRAG85 states that fault trees are only necessary for safety systems that do not have sufficient system-wide reliability data. We suggest that fault trees be developed for all safety systems.

The development of fault trees is necessary to assure that the design has eliminated all single point failures and that all potential common failures of multiple systems have been identified. The detailed examination necessary for fault tree development may also uncover unnecessary design weaknesses that may be readily eliminated.

Plant experience with system availability can be used as a check against the detailed analysis, but it should not be the basis for risk assessment. Data obtained under test conditions may not be representative of actual performance under emergency conditions. Operator errors and other intermittent failures may not be reported; the test may simply be repeated, "to make sure the test was conducted correctly."

Modular Fault Tree Analysis. RFRAG85 lists modular fault tree analysis as a methodology that is used by Safety Analysis Engineering for development of fault trees. Modular fault tree analysis is based on the use of standardized modules which model complex systems and their support system and operator interfaces. Standardization of logic structures and nomenclature for common systems or components is a desirable practice that is applicable to Rocky Flats facilities, but modular fault tree analysis is a formal methodology that is based on a computerized library of models.

The primary reference for modular fault tree analysis describes a library, but that library is designed for use in developing fault trees for nuclear power plant systems that will be analyzed using the SETS computer program.[12] As presented in the reference, the library is not applicable to Rocky Flats.

The modules in the primary reference might be obtained from Sandia National Laboratories, modified to represent Rocky Flats systems, and converted to a format compatible with FTAP or other fault tree software to be used at Rocky Flats. The models would have to be reviewed and revised as necessary to reflect typical Rocky Flats installations. Additional modules would have to be created to model systems that do not appear in nuclear power plants, but are common at Rocky Flats, such as glove boxes and HEPA filtration systems. The nomenclature scheme would have to be revised, preserving uniqueness of event trees and maintaining correct linkage, and the revised nomenclature scheme should be documented in a revision to RFRAG85.

However, we suggest that the formal modular approach be abandoned for Rocky Flats. Unlike nuclear power plants, Rocky Flats has few similar sites that could share the cost of developing a

module library. The limited benefits available from the use of this methodology do not appear to justify the investment necessary to develop the library of modules.

Top-Down Approach. Section 2.3.3.3 of RFRAG85 lists "Immediate Cause Method" as an optional methodology for use in developing fault trees. As described in RFRAG85, the Immediate Care Method is the usual top-down procedure for developing fault trees. Failure to use this method would be a significant deviation from generally accepted practice and would reduce confidence in the results of the risk assessment.

Common-Cause Failures. The plant-specific data may indicate potential common-cause relationships that are not included in the bulleted list given in Section 2.3 of RFRAG85. All potential common-cause failures should be reflected in the fault tree, regardless of whether the actual cause can be identified.

Guidelines. Section 2.3.2 of RFRAG85 suggests simplifying assumptions that appear to have been adapted from the procedures for performing an Interim Reliability Evaluation Program (IREP) analysis.[13] The objective of an IREP analysis was preliminary identification of dominant accident sequences in nuclear power plants as a foundation for subsequent risk assessment. No such simplification should be used in a final safety analysis at Rocky Flats without a detailed justification.

We suggest that RFRAG85 be modified to include specific guidelines that would standardize minor features of the fault tree, thereby causing errors in draft versions to stand out more prominently and generally making the trees easier to read and understand. The guidelines might include procedures to follow in developing a fault tree. Appendix B suggests some guidelines for fault tree development.

Qualitative Fault Tree Analysis. Section 2.3.4 of RFRAG85 describes a procedure for merging of support and safety systems into one fault tree before obtaining minimal cut sets. We recommend that the safety system fault trees be separately analyzed as they are developed, to check for single-point failures and unexpected double failures.

DOE Order 6430.1 requires that safety class systems be designed to perform their safety function with the imposition of a single failure (defined in the order).[11] Therefore, any such single-point failure would be sufficient to disqualify the design of a facility addition or alteration.

4.5 Reliability Database Development Methodology

Integration of Human Errors Into Methodology. Section 2.4.1 of RFRAG85 treats the identification of human interactions as if the procedure were an add-on to an already completed risk assessment that did not include human failures. In fact, potential human errors should be considered throughout the analysis. The PHA should include examination of operating, test, maintenance, and emergency procedures, as well as training and certification pertaining to safe operation and maintenance. The FMEA should include operator and maintenance failure modes and their effects. Potential human errors should be considered in any top-down top-level analysis and in the development of IELDs. Any satisfactory method for development of fault trees will identify potential human faults unless the analyst specifically excludes them.

Table 2.4-1 of RFRAG85 omits any measure of uncertainty or any other indication that the frequency of a human error will be assigned a probability distribution. Each failure rate should be assigned an error factor or the equivalent. In fact, there seems to be little reason to describe separate procedures for human and component reliability data bases. The only major differences are the sources for generic data. The remainder of this section contains a review of the methodology for developing a

component reliability database and makes recommendations for improvements. Those discussions and recommendations apply to the human failure rates as well.

Scope of Reliability Database. The approach described in Section 2.4.2 of RFRAG85 assigns failure rate or unavailability distributions directly to the basic events. Current practice is to identify classes of basic events that would each include events expected to have the same frequency. A database is created to contain the failure rates and/or unavailabilities for those events. Each individual basic event is assigned to one of the classes and thereby receives a failure rate or unavailability.

This approach permits tracking of multiple appearances of an uncertainty arising from one failure rate estimate. The correlation of these uncertainties increases the mean accident frequency. Therefore an analysis that neglects such correlations may not be a bounding analysis.

Recent Sources. RFRAG85 might be updated to include more recent sources for generic data. For hardware items, the IAEA publishes a useful compendium of nuclear power plant data.[14]

Page 8-6 of the 707FSAR says that the mitigating system failure and success probabilities are calculated by fault tree analysis or estimated by a "modified Delphi approach using current operating conditions, plant response capabilities, operator's experience, and engineering judgments." It could be concluded from this that generic equipment failure rates and human error rates that are well-documented in the literature and available when the FSAR was produced may not have been used to predict the accident scenario frequency in many of the cases treated to analysis. This could account for the very low frequencies predicted in the FSAR when human error was involved in the accident sequence.

Plant-Specific Data. The discussion in Section 2.4.2 of RFRAG85 is not clear on the use of the word "component." A "generic database" is organized by failure modes of generic components, with "generic failure rates" based on data from a variety of sites (but perhaps only one type of plant). A "plant-specific database" provides failure rate estimates that are specific to one site, but the estimates are still organized by failure modes of generic components.

With the above clarification, the methodology for obtaining plant-specific failure rates is applicable to Rocky Flats, and plant-specific data should be sought for each database entry. However, compiling good plant-specific data may consume considerable resources and may not be necessary for a bounding analysis. The examination of plant experience for a particular failure rate need only be sufficient to detect any trend toward higher rates at Rocky Flats and be sufficient to provide a basis for estimating the uncertainty in the plant-specific rate.

Note that Page 8-62 of the 707FSAR has the following statement: "The Fault tree/Event tree data used to calculate operational accident risks are based on generic component and human error failure rates and documented uncertainty ranges. If manufacturer's reliability data for a specific component are available, or a detailed human factors engineering evaluation is performed to identify and quantify human error rates, the operational accident risks are expected to be several orders of magnitude higher." Are we to conclude from this that risk analysis results calculated from fault/event tree data are too low by several orders of magnitude? If so, that would apply to virtually all of the results documented in the FSAR.

Logarithmic Distributions. The restriction to lognormal or loguniform distributions (Section 7.3 of RFRAG85) is satisfactory provided that the distributions are shown to bound the actual distributions, particularly at the high-frequency end.

External Event Frequencies. We suggest that the database include frequencies of various external events, by severity level. Each frequency should be represented by a probability distribution, expressing the uncertainty in the frequency.

4.6 Accident Frequency Quantification Methodology

Calculation of Accident Frequencies. In Section 2.3.4 and 2.3.5, RFRAG85 describes a four-step process for calculating frequencies, using the large-fault-tree approach. Two or three of the steps appear to be performed by computer software. The first step is the merging of support and safety systems into one fault tree for each event tree heading, resulting in a set of Boolean equations. To say, as RFRAG85 does, that this checks the draft fault tree for "accuracy" seems to be too strong. "Consistency and completeness" may be a more apt description of the qualities that could be checked by this process.

The second step, apparently manual, uses the result of the previous process to prepare input for the FTAP computer model. In the third step, the FTAP code obtains minimal cut sets. Finally, a computer file created by FTAP is used as input to the IMPORTANCE code, which quantifies the large fault tree. The IMPORTANCE code also requires reliability data, which are apparently prepared manually.

This methodology is not applied to external events. Instead, the quantification is based on the Design Basis Earthquake (DBE), Wind (DBW), and Tornado (DBT), used in this context to refer to the most severe such events applicable to the site. It should also be noted that these event severities were not necessarily the original basis for the design of each building.

Earlier analyses indicated that structural capacities of various specific buildings are less than the loads cause by Design Basis events. The LATA reports (e.g., RF006360[01]) estimate various "conservatism factors" and produce various realistic (higher) capacities for threshold and total damage. These realistic capacities are mean values (buildings may be stronger or they may be weaker).

It is cause for some concern that the estimated conservatism factor conveniently turn out to yield "Realistic Capacity" for the Building 707 complex that is apparently adequate for the design basis wind and tornado (except wind-driven missiles). After removal of conservatism factors, "realistic" earthquake levels for the Building 707 complex range from less than the DBE to greater than the DBE.

The LATA reports are referred to in RFRAG85 (e.g., Pages 34 and 36) but not listed in the references. The LATA reports are cited in "Risk From Natural Phenomena Events for Existing Plutonium-Handling Facilities at the Rocky Flats Plant," prepared by Safety Analysis Engineering, July 1986. This report is also not cited in RFRAG85, though it appears to be intended to supplement RFRAG85.

Uncertainty Propagation. According to Sections 2.5.1 and 7.4.2 of RFRAG85, the propagation of uncertainty is not done with the large fault tree. Instead, the IMPORTANCE code propagates uncertainties through fault trees by the Monte Carlo method. Uncertainty is propagated through event trees using the method of moments, perhaps by hand.

RFRAG85 provides no guidance to the accuracy to be demanded of the Monte Carlo procedure. It is important that the calculated distribution be either accurate or else a bound on the actual distribution, especially at the high-frequency end. Monte Carlo methods do not normally provide any accuracy at the tail of the distribution unless they are biased to concentrate on the tail.

The original IMPORTANCE methodology did not calculate uncertainty.[15] Chapter 7 of RFRAG85 is not clear on whether the IMPORTANCE software configuration being used by Safety

Analysis Engineering includes the effects of correlated uncertainty (failure rates from the same source). Although Table 2.4-2 suggests that distinction between median and mean is noted, Section 2.5 of RFRAG85 fails to say which is reported when a central value is given for frequency.

Apparently propagation through event trees ignores correlations in uncertainties. If so, the calculated frequency distribution may not be an upper bound.

Uncertainty analysis has been an area of active research during the 1980s. We suggest that the FSARs provide greater detail of the methods used for uncertainty analysis. This would include how events were grouped for correlated uncertainty, the number of Monte Carlo trials, and the number of moments carried in the analysis.

The approaches described in RFRAG85 may be valid if they include an acceptable treatment of uncertainty and they are executed correctly. The required analysis is complex, but it is within the current state of the art.

Quality Assurance. RFRAG85 and the FSARs provide no assurance of the accuracy of the analysis tools. Neither do they provide any assurance that the manual procedures were followed correctly. The evaluation being reported here did not include independent verification and validation of the particular software configurations that were used to prepare the FSARs.

To provide for independent review of the FSARs, we suggest that they include supporting documentation of quality assurance procedures that were applied to the software and to the software input and operation. We also suggest that sufficient intermediate results be given to permit independent tracing of the entire quantification process.

Success Fractions. Event tree branches have split fractions that assign a probability to each branch. Usually one branch is a system failure and the other is system success. Section 2.5.2 of RFRAG85 suggest two methods for obtaining the probability of system success.

However, unless there is *a priori* knowledge that one branch has both greater frequency and greater consequence than the other, a bounding analysis must use upper bounds for each split fraction. Although the sum of the actual split fractions will be one, the sum of the upper bound split fractions will generally be greater than one. In fact, we suggest that a split fraction of 1.0 be assigned to any success branch because that will usually not be much greater than the actual split fraction.

Screening. The RFRAG85 is correct in cautioning against assuming that risk of low frequency events will be acceptable. To maintain assurance that the analysis bounds the total risk, the frequencies of "incredible" events (Section 8.3.1) may be totaled and assigned to the maximum credible consequence (Section 8.3.2).

Similarly, the risk assessment should not accept a design assumption that the risks from accidents larger than DBA are acceptable (Section 8.3.1). The purpose of safety analysis is to check the design assumptions, and the probabilistic risk assessment should explore the entire frequency space. Here, again, the risk of larger accidents may be bounded by determining an upper bound on their frequency and assigning the maximum credible consequence.

Page 2-6 of the 707FSAR, states that boundaries of the analysis include the cutoff of accident scenarios below the level of credibility as defined by a frequency of 1 E-6 per year and of not considering the impact of natural phenomena events above design basis levels. There is no clue in the FSAR as to how uncertainty was treated when rejecting further consideration (or documentation) of scenarios considered and then discarded because the estimated frequency of occurrence was below the cutoff. Additionally, Page 2-6 of the 707FSAR, says that the radiological dose to an off-site individual

exceeds the DOE guidelines at a frequency of once per 8000 years. There is also no clue as to how uncertainty was considered when deriving this statement.

Page 8-2 of the 707FSAR states that for accident scenarios having high consequences, but a predicted frequency of occurrence less than the cutoff frequency (1 E-6), they are "considered" because of the large uncertainties involved in such an analysis. It is not clear what this means.

Iteration. Section 2.5 of RFRAG85 describes a separation of quantification into two stages, the first using generic data and the second using improved or plant-specific data for dominant sequences. This is a good approach for interim analyses during design of a new building or modification of an existing building.

However, because there are many buildings and processes to be analyzed at Rocky Flats, plant-specific data will ultimately be needed for most failure rates. Once these data have been developed, there is no reason to use generic data in other analyses. In particular, FSARs should be based on the best available data.

Uncertainty in Prior Estimates. Section 7.4.2 of RFRAG85 suggests that literature values of failure rate uncertainty (which are reported as covering 90 percent of the population) be interpreted as including only 80 percent of the population. We concur with this conservative practice because it mitigates the tendency of expert panels to underestimate the uncertainty of their predictions.

5. ACCIDENT CONSEQUENCE ANALYSIS METHODOLOGY

5.1 Energy Release Damage Analysis Methodology

Fault Trees for External Events. Chapter 3 of RFRAG85 makes no mention of applying fault trees to external initiating events. In fact, fault trees should be applied to these events as well as to operational accidents. There is a distinct overlapping of external events and operational failures.

Combustion. The subject of fires is only briefly addressed in RFRAG85 (see Page 10). It appears that the intent with respect to fires of various types, as indicated in implementation of RFRAG85 in FSARs, is to use historical data on fire incidents, coupled with an arbitrary "improvement factor" of ten. The Building 771 FSAR references RFRAG85 and applies an "assumed improvement factor of 1E-1" for fire inside incinerator gloveboxes (Page 8-11), fire in small furnace operations (Page 8-12), and fire in noninerted gloveboxes (Page 8-12). We suggest that each category of fire be analyzed with fault tree methodology to define each factor and probabilities that led to occurrences of fire, instead of using an arbitrary adjustment of historical data.

Multiple Phenomena. RFRAG85 ignores the potential for accident sequences with multiple energy release, such as explosion followed by fire and *vice versa*. We suggest that event trees be extended to include all phenomena that can occur before the situation is stabilized.

5.2 Contamination Damage Analysis Methodology

Sources of Contamination. We suggest that the methodology be extended to include determination of upper bounds for non-radioactive contamination, especially toxic chemicals.

Material-at-Risk. Section 3.1.3 of RFRAG85 defines material-at-risk as "material that is in jeopardy from impacts caused by falling/blowing debris and is subject to resuspension from ambient winds." It states that material stored in sealed cans is generally not at risk, and merely taping on a lid constitutes "sealed." It does not appear to be reasonable to assume that collapse of building with heavy concrete panels, plus the possibility of fire, will not cause the rupture or lid separation on at least some of the containers, increasing the amount of material-at-risk. Section 3.1.3.1 says that the material-at-risk really isn't all at risk. An "inventory availability" (material actually at risk) is obtained by multiplying the material-at-risk by a residence time factor. We suggest that detailed consideration of material-at-risk be deferred to the next chapter in RFRAG85, where the source term for both operational accidents and external events is characterized.

Damage Ratios. In Section 3.1.4 of RFRAG85, a "damage ratio" is from the LATA assessment and is "either the percentage of gloveboxes crushed by falling debris or perforated such that two unfiltered openings are created." The LATA assessment provides estimates of damage levels in categories of "minor, moderate, and heavy," and does not address the number of openings created. Only one unfiltered opening can result in release in the presence of varying wind velocities or fire. One value of "damage ratio" applied to a given building for a given scenario appears to be too simplistic to be credible; appropriate damage levels can be evaluated for various parts of a building by use of branches in event trees. RFRAG85 confuses the procedure by confusing the term "damage ratio" with the concept of "release fraction" in Chapter 4. We suggest that the treatment of "material-at-risk" and applying a simple "damage ratio" to define a source term is out of place in Chapter 3 (external events) and should be left to an expanded characterization of the source term in Chapter 4.

Source Terms and Release Factors. Characterization of the source terms in Chapter 4 of RFRAG85 should incorporate considerations presently in Chapter 3 on external events. The "material-at-risk" in Section 4.4.1 apparently should include the "residence time factor" introduced in Chapter 3.

The effect of a sequence of environments does not appear to have been considered. Page 8-21 of the 707FSAR describes an accident in which a ventilation system failure causes overpressurization of a glovebox(es) leading to release of contamination. The accident sequence does not continue with restoration of ventilation pressure and the consequent inrush of room air causing a glovebox fire. A realistic assessment would consider the occurrence of such obvious results of the postulated initiating event. Another area of concern is the treatment of the earthquake scenarios at different lateral accelerations as discussed beginning on Page 8-39. The scenarios typically result in leak of contamination from damaged gloveboxes and exhaust ventilation ducts in the inert ventilation system. The accident scenarios do not appear (except for the most severe earthquakes) to include the possible scenario of burning plutonium caused by loss of inert atmosphere as another mechanism for dispersal and increasing the inhalable source term. Page 8-45 discusses the dispersal of plutonium from the rubble pile where modules J and K were before the earthquake. There appears to have been no consideration of enhanced dispersal owing to chemical reaction between the material in the storage vaults with either water or carbon tetrachloride released from their respective piping and storage systems by the same earthquake. These are examples of nonconservative truncating of the accident sequence by the analysts responsible for producing the data from which the FSAR was produced.

Material Transport and Aerosols. According to RFRAG85, the TVENT1P and MSPEC codes are applied to flows and depositions within an intact HVAC system during passage of a tornado. It is not clear how this contributes to a release from a building unless there are associated HEPA filter failures.

Page 8-45 of the 707FSAR states that, for a catastrophic earthquake, the source term for modules A through H is negligible since the leakpath occurs through the exhaust ventilation system by natural circulation and all effluent is filtered. A proper risk assessment should include scenarios where: filters are damaged or bypassed, other leakpaths are created by the earthquake, winds defeat the natural draft, etc. All of these other scenarios are credible and may be of significant likelihood. 707FSAR Page 8-54 states that the same release fractions were used for extreme winds as was used for earthquakes. The inference is that the consequential structural damage determines the release. This is non-intuitive in that, subsequent to the structural damage, persistence of high winds may significantly increase the rate of dispersal by blowing briskly through the damaged building and the rubble.

In the presence of structural failure, an atmospheric exchange method is described (Section 5.2.4). A methodology for getting from the LATA damage assessments (minor, moderate, or heavy) to input to the somewhat complex release equations in Table 5.2-1 is not provided. The expulsion of material from a glovebox when crushed (as with a bellows blower) is not mentioned.

Under Section 5.3.2, dealing with deposition factors, it states: "For particulates less than 10 uum in diameter, a removal factor of 1.0 is recommended." (Here "u" represents "mu.") If this means "10 micro-micron," it would represent only 0.1 Angstrom, surely a much smaller diameter than would be considered If it is intended to be "1-micron-squared in area," it would correspond to 3.6 micron in diameter.

Dispersion and Consequence Analysis. As described by RFRAG85, the TRAC code calculates plume concentrations and surface depositions and resuspensions in various zones around the facility. The code then calculates population doses (Section 6.1.6) from inhalation and air-shine from the passing plume, inhalation from resuspension of deposited materials, ground-shine from deposited materials, and ingestion of foods and drinking water contaminated by surface deposition. Libraries of dose conversion factors for the several pathways were assembled from several publications and codes.

Caution is in order for interpretation of input that produced the ingestion dose conversion factors. Presumably, some sort of averaging of food crops production and consumption, population densities, surface drinking water, etc., is done in applying the PABLM code for ingestion factors that are then combined with ground-shine factors. A 50-mile radius from Rocky Flats includes much area in mountains, forests, and desert land. The concept that each person standing on a given area with an

associated deposition of radionuclides and exposed to the corresponding ground-shine, consumes food and water from that area (though he may be standing on a rock in the mountains or in downtown Denver) is not realistic. We suggest that the logic and input related to dose conversion factors be carefully reviewed.

Effects. Worker accidental dose (Section 6.3.1 of RFRAG85) uses Table 6.3-1 for "50 and 1-year integrated acute inhalation dose conversion factors." Examination of numbers in the table indicate that it is at least partially a table for chronic instead of acute exposure and is not appropriate for the stated purposes. For example, the value for "total" for 1-year commitment, solubility class Y, and 1-micron size, is 2.1 E+3. The corresponding value for 50-year commitment is 5.7 E+5, a factor of 271 greater than for one year. For a one time intake, the 50-year commitment, even if there is no physical decay and no biological decay, cannot exceed 50 times the 1-year commitment. The corresponding ratio from the table for 7-micron is 84 and for 30-micron is 42.

References

1. *Rocky Flats Risk Assessment Guide*, Safety Analysis Engineering, Rockwell International, North American Space Operations, Rocky Flats Plant, March 1985.

2. "Operational Readiness Review at the Department of Energy's Rocky Flats Plant, CO," Defense Nuclear Facilities Safety Board Recommendation 90-4, 55 FR 19644-19645, 10 May 1990.

3. "Operational Readiness Review at Department of Energy's Rocky Flats Plant, Colorado; Response to Recommendation 90-4 of the Defense Nuclear Facilities Safety Board," Department of Energy, 55 FR 25866-25867, 25 June 1990.

4. "Systematic Evaluation Program at Department of Energy's Rocky Flats Plant, CO," Defense Nuclear Facilities Safety Board Recommendation 90-5, 55 FR 21429-21430, 24 May 1990.

5. "Systematic Evaluation Program at Department of Energy's Rocky Flats Plant, CO; Response to Recommendation 90-5 of the Defense Nuclear Facilities Safety Board," Department of Energy, 55 FR 25154-25867, 20 June 1990.

6. *Safety Analysis and Review System*, Order DOE 5481.1B, U.S. Department of Energy, Washington, 23 September 1986.

7. *Safety of Nuclear Facilities*, Order DOE 5480.5, U.S. Department of Energy, Washington, 23 September 1986.

8. Joseph G. Morone and Edward J. Wookhouse, *The Demise of Nuclear Energy?*, Yale University Press, New Haven, 1989.

9. Harry F. Martz and Ray A. Waller, *Bayesian Reliability Analysis*, John Wiley & Sons, New York, 1982.

10. *Quality Assurance*, Order DOE 5700.6B, U.S. Department of Energy, Washington.

11. *General Design Criteria*, Order DOE 6430.1A, U.S. Department of Energy, Washington, 6 April 1989.

12. B. B. Varnado *et al.*, *Modular Fault Tree Analysis Procedures Guide*, NUREG/CR-3268, U.S. Nuclear Regulatory Commission, Rockville, MD, August 1983.

13. D. D. Carlson, *Interim Reliability Evaluation Program Procedures Guide*, NUREG/CR-2728, U.S. Nuclear Regulatory Commission, Rockville, MD, January 1983.

14. *Component Reliability Data for Use in Probabilistic Safety Assessment*, IAEA-TECDOC-476, International Atomic Energy Agency, Vienna, October 1988.

15. Howard E. Lambert, *Fault Trees for Decision Making in Systems Analysis*, UCRL-51829, Lawrence Livermore Laboratory, 9 October 1975.

Appendix A

Suggested Procedures for Hazard Identification

HAZOPS

HAZOPS is one of the structured methodologies available to identify process hazards and potential operating problems. The method is based on the use of a series of guide words to evaluate the sources of potential process deviation. The use of HAZOPS methodology is very prevalent in the chemical industry where the hazards and the potential initiators are varied and different between different facilities. A list of guide words, such as "High" and "Low" which when associated with another list of parameters such as "Flow" provides the analyst with a check-list to associate possible causes for estimating the sources of hazards. Additionally, the immediate consequence and the action required to mitigate the hazard are generally listed.

Preliminary Hazard Analysis (PHA)

Checklist. Section 2.1.1.1 of RFRAG85 should show the PHA checklist. In addition to the items mentioned in the RFRAG, the checklist should cover the safety design criteria to be used. This includes documentation of overall process safety success criteria, success criteria for individual systems, the bases for these criteria, and the dependencies that relate them. This information is needed to understand the potential dependencies of events in accident sequences.

The checklist should cover not only normal energy sources, but also toxic chemicals, stored fuels, combustibles, reactive chemicals, and pressure systems. The PHA should describe not only energy sources and barriers, but also sources and barriers for toxic and radioactive materials. The Rocky Flats plant differs from reactors in that there are diverse nonradioactive energy sources, whereas the radioactive material itself is not usually an energy source.

The PHA checklist should include examination of the following for identification of hazards:

- ***Safety related interface considerations among various elements of a process.*** (e.g., material compatibilities, electromagnetic interference and other possibilities of inadvertent actuation, fire/explosive initiation and propagation).

- ***Environmental constraints including the normal operating environments.*** (e.g., drop, shock, extreme temperatures, noise and health hazards, flammable gases, liquids, and dusts, cryogenic systems, high temperature systems, inert and low oxygen atmospheres, effects of chemical exposures, high intensity magnetic fields, toxic and noxious emissions, mechanical and moving equipment dangers, inadequate ventilation, working at heights, pesticide use, electrostatic discharge, high voltage, lightning, X-ray, electromagnetic radiation, and laser radiation).

- ***Operating, test, maintenance and emergency procedures.*** (e.g., human error analysis of operator functions, tasks, and requirements; effect of environmental factors such as equipment layout and lighting requirements on human performance; possible abnormal operations; potential credible accidents; accident amelioration; egress, rescue, and survival).

- ***Facilities and support equipment.*** (e.g., provisions for storage, assembly, checkout, prooftesting of hazardous systems/assemblies which may include toxic, flammable, corrosive or cryogenic fluids; electrical power sources).

- ***Training.*** (e.g.training and certification pertaining to safe operation and maintenance).

- ***Safety related equipment, safeguards, and possible alternate approaches.*** (e.g., interlocks, system redundancy, fail-safe design considerations, subsystem protection, fire suppression systems, and personal protective equipment).

Failure Mode Effects Analysis (FMEA)

Iteration. While the objective of an FMEA is to identify all modes of failure within a system design, its first purpose is the early identification of all catastrophic and critical failure possibilities so they can be eliminated or minimized through design correction at the earliest possible time. Therefore, the FMEA should be initiated as soon as preliminary design information is available at the higher system levels and extended to the lower levels as more information becomes available on the items in question.

System Definition. The RFRAG should specify that all existing process descriptions, functional block diagrams, functional sequence diagrams, technical specifications, interface specifications, piping diagrams, wiring diagrams, reliability test data, and failure reports must be examined before the FMEA is considered complete. All data, drawings and engineering notebooks generated during design should be available for reference, including corrective actions initiated and their resolution. All operation and maintenance manuals and training materials should be examined.

Analysis Approach. The RFRAG should specify a top-down functional approach to the FMEA. This is the approach normally used for the complexity that is generated by defense in depth.

Indenture Level. The RFRAG should also provide guidance for selecting the functional level at which failures will be postulated for the FMEA. Once the design has progressed to appropriate detail, the resolution should be at least to the level of the database for item failure modes and human errors. It is preferable to go to even lower levels, to assure that no hazard is overlooked. Items identified as having a catastrophic or critical failure mode should be analyzed to as low a level as possible.

Worksheet. The FMEA worksheet format should be expanded to include the unit identification (e.g., drawing and part numbers), the operational mode, and maintenance actions. For hardware items, the identification should be by hardware breakdown structure, drawing and part number, or other similar uniform numbering system. Humans should be identified by specific operation or maintenance task, individual by individual, except for functional redundancy within a team. Operational modes may include standby, startup, shutdown, test, and other modes appropriate to the facility and process, and the effects of each failure mode should reflect any dependence on operational mode. Documentation of maintenance actions is needed to assess the duration of the failure and the potential for maintenance errors.

If the failure effect is the loss of a protective feature or the loss of a redundancy, there should be an explicit statement of the system, process, or facility failure effects that have an increased probability of occurrence or a reduced probability of mitigation. This will assure that the failure mode is not overlooked when fault trees are prepared.

Failure modes and effects should be defined in terms of performance parameters and allowable limits. The example in Table 2.1.1 is deficient in this respect. What constitutes failure to close? That is, what is the limiting condition of operation (LCO) for leakage through the valve and what is the LCO for negative pressure? How is the LCO for leakage related to the LCO for negative pressure? Can the valve be within its leak rate LCO and still cause the negative pressure to exceed its LCO? Can the valve exceed its LCO without causing excess negative pressure? What is the nominal value of negative pressure for the alarm and what is its tolerance? Which of the following is the definition of "fails to close":

- Flow exceeds valve leakage LCO,
- Negative pressure exceeds its LCO, or
- Negative pressure is sufficient to trigger alarm
  - at nominal value or
  - at low end of tolerance?

What about timing? How fast must the valve close before it is considered a failure?

Severity Classification. The RFRAG should specify a standard set of effects categories, perhaps by reference to MIL-STD-1629A.[1] However, DOE Order 6430.1 requires that safety class systems be designed to perform their safety function with the imposition of a single failure (defined in the order).[2] Therefore any such single-point failure would be sufficient to disqualify the design of a facility addition or alteration.

Procedure. The following discrete steps should be followed in performing an FMEA:

- Define the facility to be analyzed. Complete facility description includes identification of internal interfaces between processes and interfaces with other facilities, expected performance at all indenture levels, process and system restraints, and failure definitions. Functional narratives of the facility should include descriptions of each process in terms of functions which identify tasks to be performed for each process, process phase, and operational mode. Narrative should describe the process environment, expected batch process times and equipment utilization, and the functions and outputs of each item. Additionally, an inventory of hazardous and potentially dangerous and toxic substances should be clearly identified.

- Construct block diagrams. Functional and reliability block diagrams which illustrate the operation, interrelationships, and interdependencies of functional entities should be obtained or constructed for each process and system in the facility. All process and system interfaces should be indicated.

- Identify all potential item (hardware and human) failure modes and all interface failure modes. For each failure mode, define its effect, by operating mode, on the immediate function or item, on the system or process, and on the facility. Identify any reduction of the degree of protection against failures of the function, item, system, process, or facility.

- Evaluate each failure mode in terms of the worst potential consequences which may result and assign a severity classification category.

- Identify failure detection methods, maintenance actions, and compensating provisions for each failure mode.

- Identify corrective design or other actions required to eliminate the failure or control the risk.

- Document the analysis and summarize the problems which could not be corrected by design and identify the special controls which are necessary to reduce failure risk.

Initiating Events Logic Diagram (IELD)

An initiating events logic diagram (IELD) analysis identifies initiating events. The structure of the IELD follows the categorization of events. For a nuclear reactor, for example, specific initiating events may be developed within the following categories: overpower, undercooling, events requiring setback and/or manual shutdown, and spurious reactor trips. The intent of the IELD is to identify specific component failures that comprise each of the categories of initiators. Development of the IELD is driven by the following considerations:

- Completeness
- Common Cause Effects
- Ease of Quantification
- Linking with Mitigating Events.

The IELD must be complete so that all credible initiating events are recognized. Incomplete identification of initiating events results in incomplete quantification of risk.

The IELD is developed in a logical manner so that common cause events are correctly considered. For example, failure of an electrical bus which affects numerous motors is a common cause event. Specific identification of all components rendered inoperable by the failure is important so that subsequent consideration of mitigating events does not take credit for components that are actually unavailable due to the initiating event.

The IELD is developed to a level of detail consistent with the database used to quantify events. It is meaningless to develop a component failure into specific subcomponent failures if data does not exist to quantify the subcomponent failures.

In the development of the IELD, it is important to understand how various events can be mitigated. Different initiating events require different systems and components to mitigate their impact. In a nuclear reactor, for example, a loss of coolant accident may render normal primary cooling unavailable while failure of thermal shield cooling does not. At a more detailed level, failure of a primary pump would render the pump unavailable while failure of an ac motor to a primary pump would not negate the ability to use the pump with its dc pony motor. This consideration of how initiating events will be linked with mitigating events is important.

Multiple independent failures of concern as credible initiating events can be easily identified once failure frequencies are assigned to the initiating events on the IELD. The process for this identification is as follows. Multiple independent failures which occur during the initiation phase of an accident are of concern; multiple failures occurring after the initiation phase during the mitigation phase are handled by analysis of the mitigating systems fault trees. The initiation phase of the accident can be defined as the time from the first failure until a mitigating system should be initiated; for most initiators, ten seconds is a conservative value. Two independent failures are of concern if their cumulative frequency exceeds some conservatively small value, typically 10^{-7}/year. The cumulative frequency is the product of two terms: the frequency of the first failure, F_1, and the probability a second

independent failure occurs within ten seconds of the first which is F_2T where F_2 is the frequency of the second failure and T is ten seconds. Thus, multiple independent initiators are of concern when

$$F_1F_2T \geq 10^{-7}/\text{year}.$$

For F_1, and F_2 in units of year^{-1} and T equal to 10 seconds, this criteria is

$$F_1F_2 \geq 0.32/\text{yr}^2.$$

A search of all combinations of independent initiating events which satisfy this criteria provides those multiple independent initiating events of concern. This technique can be refined to consider common mode failures by considering combinations where

$$F_1P_2 \geq 10^{-7}.$$

P_2 is the fraction of event 1 failures which cause event 2 due to common mode. In practice, it is difficult to apply this criterion for two reasons:

- Most initiating events are associated with operating equipment as opposed to standby equipment and as such common mode failures are more difficult to quantify.
- Only common mode failures occurring within time T (typically ten seconds) qualify as initiating events and the likelihood of a common mode failure occurring within this short interval is difficult to quantify.

These two reasons also mean that common mode initiating events (except of course those due to external initiators) are of less concern than common mode mitigating events which consider both standby equipment and a longer fault exposure time, typically 24 hours.

Digraph-Fault Tree Methodology

Section 2.3.3 of RFRAG85 suggest the use of the Digraph-Fault Tree Methodology for the development of safety and support system fault trees. We suggest this methodology be considered instead for the development of IELDs.

The digraph is a multi-valued deductive logic diagram that describes the interrelationships among process variables. It is in essence an intermediate step between the system schematic and the construction of a fault tree.

The digraph procedure was devised for failure analysis of control systems; it has been applied to safety analysis of chemical process systems and security systems. Manual fault tree techniques in general do not work well in modeling these systems because it is difficult to envision the topology from the system schematic when manually constructing a fault tree.

References

1. *Procedures for Performing a Failure Mode, Effects and Criticality Analysis,* MIL-STD-1629A, Naval Publications and Forms Center, Philadelphia, 24 November 1980.

2. *General Design Criteria,* Order DOE 6430.1A, U S. Department of Energy, Washington, 6 April 1989.

Appendix B

Suggested Procedures for Fault Tree Development

Guidelines. We suggest that RFRAG85 be modified to include specific guidelines that would standardize minor features of the fault tree, thereby causing errors in draft versions to stand out more prominently and generally making the trees easier to read and understand. The guidelines should include:

- Standard syntax for fault descriptions,
- Standard nomenclature for identifiers, and
- Standard left-right order for faults under a gate.

The RFRAG should indicate how the procedures should be followed in developing a fault tree. This might be done, in part, by reference to the following basic rules in NUREG-0492:[1]

- State precisely what the fault is and when it occurs.
- If the normal functioning of a component propagates a fault sequence, then assume that the component functions normally.
- Define all inputs to a particular gate before undertaking further analysis of one of them.

Reference

Fault Tree Handbook, NUREG-0492, U.S. Nuclear Regulatory Commission, Rockville MD, January 1981.

Appendix C

Suggested Theoretical Basis for Probability Distributions of Frequency

Section 7.1 of RFRAG85 adopts a subjective definition of probability. Martz and Waller point out that "... the subjective probabilities assigned to a particular hypothesis by one individual may be quite different from those that would be assigned by some other individual."[12] Reliance on a subjective definition subjects a risk analysis to the criticism that its risk bounds are based on subjective judgements by the analyst. Therefore, the argument might proceed, the calculated risk bound may not represent the risk bound that would be determined by other knowledgeable individuals, such as officials of the DOE, members of a DOE advisory board, or experts representing the interests of the general public.

Instead, probability might be defined objectively in terms of a nested collection of experiment spaces. Each experiment space consists of trials. In the present context, a trial is the operation of a specific facility under specific time-dependent operating conditions. Operating conditions include the external physical environment, the production levels of the facility, and the facility management (hiring policies, manuals, operator training, etc.)

The smallest such experiment space would contain just one trial; that is, an actual Rocky Flats facility with its actual time-dependent operating conditions. This trial has a deterministic consequence, although unknown in advance. It is not meaningful to talk of probability or frequency for a one-trial experiment space.

A larger experiment space corresponds to the concept of "fundamental" reliability. This "fundamental" experiment space contains many facilities, all constructed to the same specifications and with the same facility management. However, they may have different histories of physical environment and production levels, representing the expected uncertainty in external events and inventory.

Each trial in the fundamental space has a consequence. The variability of these consequences is referred to in RFRAG85 as the "variability fundamental to the phenomenon being studied." The result of actually doing such an experiment would be a single risk curve, showing for each consequence, the frequency of trials that yield at least that consequence.

No PRA methodology can distinguish among the facilities and managements in the fundamental space. In fact, because a PRA is based on approximate models, there are infinitely many other fundamental spaces, representing other possible facilities and managements, that would not be distinguished by the PRA methodology. We may define the "model" space as the collection of all fundamental spaces that would fit a given model. Given a particular facility of interest, the model space that includes its fundamental space will depend not only on the facility, but also on the PRA methodology.

Each of the fundamental spaces in a model collection has its own risk curve. These infinitely many risk curves may be represented by percentile risk curves, such as those in Figure 7.1-1 of the RFRAG. For any given consequence, the p=.75 curve may indicate the 75th percentile of the values of the risk curves at that consequence.

Furthermore, a bounding analysis does not identify the percentile risk curves, it only bounds them. That is, adding any further detail to the analysis should never increase those curves.

This interpretation is objective and deals directly with the question that concerns the public. If we allow the technical community to construct and operate all sorts of facilities under its proposed standards of safety analysis, how often might we have problems and how bad might they be?

DATE
FILMED
5/23/94
END