APPENDIX B
QUALITATIVE CRITERIA FOR EVALUATION OF LIKELIHOOD

Purpose

This appendix provides additional guidance on the use of qualitative criteria in methods for evaluation of likelihood. These evaluations are used in demonstrating compliance with the performance requirements of Title 10 of the Code *of Federal Regulations* (10 CFR) 70.61, "Performance Requirements."

Introduction

The regulation in 10 CFR 70.61(b) requires that the risk of each credible high-consequence event be limited by ensuring that upon implementation of engineered or administrative controls, the event is made highly unlikely or its consequences reduced to less than high consequence. This regulation similarly requires that the risk of each credible intermediate-consequence event be limited by ensuring that the event is made unlikely, or its consequences reduced. Rather than defining the terms "highly unlikely," "unlikely," and, "credible," 10 CFR 70.65(b)(9) instead states that the applicant must include definitions of these terms in its integrated safety analysis (ISA) summary.

As stated in Section 3.4.3.2(9) of this Standard Review Plan (SRP), the applicant's definitions of these terms may be either quantitative or qualitative. The method used to evaluate accident sequence likelihood must be consistent with the definitions. Quantitative definitions require quantitative methods; qualitative definitions require qualitative methods. Qualitative methods are based on objective qualitative criteria and characteristics of the process or system being evaluated. In addition, some methods (semiquantitative methods) may rely on a mixture of qualitative and quantitative definitions, methods, and information. This appendix provides general guidance on the use of qualitative methods for evaluation of likelihood. However, the U.S. Nuclear Regulatory Commission's (NRC's) review of recently submitted ISA Summaries has revealed a lack of common understanding as to what constitutes an acceptable qualitative method.

Additional guidance is provided on the acceptance criteria for qualitative methods of evaluating likelihood, both for the failure of items relied on for safety (IROFS) and for accident sequences as a whole. Either external events or internal events (which may or may not be IROFS failures) may initiate these accident sequences. Appendix D to Chapter 3 of this SRP provides additional guidance on the use of initiating events that are natural phenomena. Appendix C to Chapter 3 offers additional guidance on the use of initiating events that are internal to the facility. That guidance may be used with the guidance in this appendix as an acceptable qualitative method for likelihood evaluation.

Discussion

Definitions of Likelihood

According to 10 CFR 70.65(b)(9), the ISA Summary must define the terms "unlikely," "highly unlikely," and "credible." Section 3.4.3.2(9) of this SRP states that qualitative definitions of likelihood are acceptable if they meet two conditions: (1) they are reasonably clear and based

on objective criteria and (2) they can reasonably be expected to consistently distinguish accidents that are highly unlikely from those that are merely unlikely (or not unlikely). This means that the definitions should be sufficiently clear that there is reasonable assurance that they will yield the same result when applied by different reviewers and that they can be used to make meaningful distinctions between events in different likelihood categories. Both the definitions of likelihood and the methods for likelihood determination should meet these criteria since they must work together to ensure that the performance requirements are met.

This NUREG states that "objective criteria" means that the method relies on specific identifiable characteristics of a process design, rather than subjective judgments of adequacy. Because the likelihood of an accident sequence is a function of the likelihood of the initiating event, the subsequent IROFS failures, and the relationship between the IROFS (e.g., whether the IROFS are independent), the characteristics of the process design that the method should rely on are the specific identifiable characteristics of the initiating event, IROFS failures, and other process features, including initial conditions, bounding assumptions, and design features that affect the likelihood of the accident sequence. These features include the safety margin, type of control, type and grading of management measures, whether the system is fail-safe or failure is self-announcing, failure modes, demand rates, and failure rates for individual IROFS (whether credited as part of the initiating event or subsequent failures). These features include the degree of redundancy, independence, diversity, and vulnerability to common-cause failure for systems of IROFS. The following sections describe these features in detail. It is important that any features of the process or equipment necessary to meet the performance requirements , including initial conditions, bounding assumptions and design features, are recognized as important to safety and are maintained in the ISA records and are included in the Configuration Management system for the facility.and ~~appropriately maintainedthrough~~ the use of other management measures as appropriate.

Comment [c1]: Text that is highlighted in blue is unchanged. This test is highlighted imply to draw attention to areas that already relate to the issue of "design features" and the fact that "initial conditions" and "bounding assumptions" may impact the likelihood of an accident sequence.

Examples of acceptable qualitative definitions of likelihood are the second and third definitions of "not credible" in Section 3.4.3.2(9) of this SRP:

> A process deviation consists of a sequence of many unlikely human actions or errors for which there is no reason or motive....
>
> A convincing argument exists that, given physical laws, the process deviations are not possible, or are unquestionably extremely unlikely....

Comment [c2]: Draw a relation ship between deviation and "safeguards" or controls. Versus the aspects of a design feature---e.g. bundle type or tank diameter…

Similarly, the following is an example of an acceptable qualitative definition of "highly unlikely":

> a system of IROFS that possesses double-contingency protection, where each of the applicable qualities is present to an appropriate degree

In this definition, the qualities to be considered should be described in sufficient detail so that their effect on the overall likelihood can be evaluated. This is the meaning of "present to an appropriate degree." Other definitions are acceptable provided that they meet the two criteria specified above and provide system features to ensure that the likelihood is appropriately maintained.

Evaluation of Likelihood

Accident sequences, in general, consist of an initiating event followed by one or more subsequent events. The likelihood of an accident sequence is, therefore, a function of the likelihood of the individual events making up the accident sequence and the relationship between them (e.g., whether they are independent). Because the likelihood of the accident sequence must be compared to the likelihood definitions to determine whether it is "unlikely," "highly unlikely," or "not unlikely," qualitative methods of likelihood evaluation are acceptable if they (1) are reasonably clear and based on objective criteria and (2) can reasonably be expected to consistently distinguish accidents that are "highly unlikely" from those that are merely "unlikely." The likelihood definitions establish the standard for what is "unlikely" and "highly unlikely," and the assigned likelihood for the accident sequence is then compared to this standard. As mentioned above, the method must take into account all objective qualities of the system that can reasonably be considered to affect likelihood. These qualities are referred to in this NUREG as the "reliability and availability" qualities of IROFS or systems of IROFS.

Initiating Events and Initial Conditions

Each accident sequence begins with an initiating event. An initiating event may consist of an external event (including a natural phenomenon or external manmade event), an internal event other than an IROFS failure, or an IROFS failure. Natural phenomena may include heavy rains, winds, flooding, earthquakes, and fires. External manmade events may include impacts from nearby facilities, aircraft or vehicle crashes, fires, and loss of offsite utilities. Internal events other than IROFS failures may include spills, non-IROFS equipment failure, process deviations, industrial accidents, and loss of onsite utilities. In a qualitative method of likelihood determination, a qualitative score is associated with the initiating event based on its objective qualities. The score may be expressed in either numerical (e.g., -1, -2, -3) or nonnumerical (e.g., A, B, C, D) form but is still qualitative if based on qualitative criteria.

The likelihood of external initiating events (by definition, they are outside the control of the facility) does not rely on any design features of the facility or process and is thus characterized only by a frequency of occurrence. In a qualitative method for assigning likelihood to these events, a qualitative score is associated with the external event based on its frequency of occurrence. Events with the same frequency of occurrence should have the same score regardless of the type of event or severity of its consequences. The method should thus include a table of the scores assigned based on qualitative frequency criteria. These criteria may include qualitative descriptions of frequency, such as "100-year flood" or "1,000-year earthquake," or may include other qualitative criteria that can be correlated to a frequency, such as "design-basis earthquake" or "exceeds the mean annual rainfall by a factor of x." By contrast, quantitative or semiquantitative methods may include quantitative descriptions of frequency such as "having a frequency less than 10-2 per year." Because these events are beyond human control, no features have to be maintained to ensure the continued validity of the assigned likelihood. However, it may be necessary to periodically reexamine the basis of these likelihoods if it is reasonably expected that the likelihood could change (e.g., following construction of a new railroad spur next to the facility). Appendix D to Chapter 3 contains additional guidance applicable to initiating events that are natural phenomena.

By contrast, the likelihood of internal initiating events other than IROFS failures depends on specific, identifiable characteristics of the facility or process design, such as those discussed in the following sections. Scores may be assigned to such events based either on objective evidence of their frequency of occurrence or on specific identifiable characteristics of the facility

or process that can affect the frequency of occurrence. If the actual frequency of occurrence is known, this information should be used as it represents objective knowledge about the event likelihood and accounts for the cumulative effect of all characteristics that can affect likelihood. Otherwise, the features of the facility or process design that can affect the likelihood should be described. Regardless of the method used to assign a likelihood score, care must be taken that all facility and process features , including initial conditions, bounding assumptions and design features, that can affect the event likelihood (reliability and availability qualities) are recognized as such and are maintained in the ISA records and are included in the Configuration Management system for the facility.~~appropriately maintained.~~ Appendix C to Chapter 3
contains additional guidance applicable to internal initiating events other than IROFS failures.

Similarly, the likelihood of internal initiating events that are IROFS failures also depends on specific, identifiable characteristics of the facility or process design. Scores may be assigned to such events based either on objective evidence of their frequency of occurrence or on specific identifiable characteristics of the IROFS that can affect the frequency of occurrence. If the actual frequency of occurrence is known, this information should be used. Otherwise, the features of the IROFS that can affect the likelihood should be described. Regardless of the method used to assign a likelihood score, care must be taken that all IROFS attributes that can affect the event likelihood (reliability and availability qualities) are recognized as such and are maintained in the ISA records and are included in the Configuration Management system for the facility.~~appropriately maintained.~~ The following provides guidance on specific reliability and availability
qualities associated with individual IROFS.

For both types of internal initiating events, facility or process features (or physical and chemical phenomena) that can affect the initiating event likelihood may be identified as initial conditions or bounding assumptions. The important factor is that these initial conditions, ~~and~~ bounding assumptions, and design features must be identified and, if susceptible to change over the lifetime of the facility (such as through process deviations or facility changes), must be are maintained in the ISA records and are included in the Configuration Management system for the facility.~~appropriately maintained~~. For example, the maximum throughput or inventory in a process may change; thus, measures should be in place to maintain this throughput or inventory if it is relied on to meet the
performance requirements, whereas the flow of gravity or maximum density may not require specific controls.

Individual IROFS

Section 3.4.3.2(9) of Chapter 3 of this NUREG states that the reliability and availability qualities of individual IROFS include (1) safety margin in the controlled parameter, (2) the type of IROFS (passive or active engineered, simple or enhanced administrative), (3) the type and safety grading of any management measures, (4) whether the system is fail-safe, failure is self-announcing, or the IROFS is subject to periodic surveillance, (5) failure modes, (6) demand rate, and (7) failure rate. It is very important that any qualitative (or quantitative) method of likelihood evaluation consider all applicable IROFS attributes that could affect the reliability and availability of the IROFS, such as those discussed below. For example, reliance should not be based solely on the type of IROFS (passive engineered, active engineered, simple administrative, or enhanced administrative).

In addition to those reliability and availability qualities discussed above, other factors may require consideration. For example, environmental conditions, such as extreme temperatures and pressures, corrosive atmosphere, excessive vibration, may have a significant effect on IROFS reliability and should be appropriately considered.

The level of detail describing the IROFS in the ISA Summary is also important. It would be acceptable to describe the IROFS at the system level if that is sufficient to demonstrate compliance with the performance requirements. The regulation in 10 CFR 70.65(b)(6) states

that IROFS should be described "in sufficient detail to understand their functions in relation to the performance requirements." It is important that the description be sufficiently detailed to identify all attributes of the IROFS that can affect its likelihood of failure, as well as everything that is within the boundary of the IROFS. It may not be necessary to specify the model number or exact design of a pump if the only attribute relied on to meet the performance requirement is the pumping capacity or oil reservoir volume. It may be sufficient to describe the pump as "centrifugal pump limited to less than 10 liters oil." The IROFS boundary includes everything necessary for the IROFS to perform its intended safety function. For example, the boundary of an enhanced administrative IROFS includes all instrumentation (sensors, annunciators, circuitry, any controls activated by the operator) relied on to trigger the operator action; the boundary of a simple administrative control includes the equipment necessary to correctly perform the action; and the boundary of an active engineered control includes the attendant instrumentation, sensors, essential utilities, and any auxiliary equipment needed to perform its safety function. The reliability and availability qualities of every component within the IROFS boundary must be considered in evaluating the total IROFS likelihood.

Additional guidance on some of the specific reliability and availability qualities of individual IROFS is provided below.

Safety Margin in Controlled Parameter: "Safety margin" refers to the difference between the value of a parameter likely to be encountered during normal or credible abnormal conditions and the value that would allow an accident to be possible. The precise value of the margin in terms of the parameter is not meaningful; rather, for the event to be unlikely or highly unlikely based on safety margin, the margin should be several times larger than the expected process variation or uncertainty. Similarly, if the margin is much greater than the change in the parameter resulting from the worst case credible upset, this fact could be credited for ensuring that the event is unlikely or highly unlikely.

The phrase "controlled parameter" indicates that means should be provided to ensure that the safety margin is continuously present, if the margin is relied on in evaluating likelihood. Parameters that are not controlled should be considered to be at their worst case credible values.

Type of Control: Passive engineered controls are generally considered preferable to active engineered controls, active engineered controls preferable to enhanced administrative controls, and enhanced administrative controls preferable to simple administrative controls. This is because, ordinarily, passive engineered controls are the most reliable, and simple administrative controls are the least reliable. Although this is one of the factors that should be considered, evaluations of likelihood should not rely solely on the type of control. This is

because the likelihood associated with passive engineered controls, for example, can vary widely depending on specific attributes of the IROFS.

Type and Safety Grading of Management Measures: The specific management measures applied to an IROFS can have a significant effect on its overall likelihood. Of particular importance is surveillance, because this can have a direct and transparent effect on the duration of failure in a method that gives credit to duration of failure. It may not be necessary to specify the frequency of preventive maintenance, testing, and calibration quantitatively in the ISA Summary. For example, to take credit for generic failure rates for a piece of equipment, it may be sufficient to specify that maintenance will be performed at a frequency and in a manner consistent with the manufacturer's recommendations. Functional testing should be conducted

in a manner that ensures that everything within the IROFS boundary is working as needed for the IROFS to perform its safety function.
While the degree and type of management measures can increase or decrease the likelihood score associated with an IROFS, primary reliance should be on designing IROFS that have a certain reliability and then applying management measures to maintain that reliability. It should not be supposed that one can achieve any desired reliability by applying increasingly stringent management measures.

Fail-Safe or Self-Announcing: This is the characteristic of an IROFS that determines the degree to which failure of an IROFS is detected and appropriately corrected. For the purpose of the ISA and ISA Summary, an IROFS is considered to fail only when it fails to perform its intended safety function. Thus, a valve that is an IROFS is not considered to fail in the context of the accident sequence (i.e., to contribute to the progression of an accident sequence) as long as it fails in a safe configuration (fails-safe). If the valve is designed to fail closed (and closed is the safe configuration), credit may be taken for the fact that the valve is designed to fail closed. The likelihood thus is not the likelihood that the valve fails, but the likelihood that it fails in a way other than how it is designed to fail. An IROFS that is fail-safe may include within its boundary a system designed to put the process into a safe condition upon failure of a component. An IROFS whose failure is self-announcing is one in which failure is either self-revealing (e.g., by presence of solution on a floor where operators are continuously present) or results in an alarm to alert operators. The main effect for the ISA Summary is to limit the duration of failure by ensuring that the upset condition is corrected essentially immediately. Similarly, surveillance may be relied on to limit the duration of failure to a specified period.

Failure Modes: In addition to specifying the safety function that an IROFS must perform, it is necessary to consider the specific failure modes of the IROFS. A particular IROFS may be credited in several different accident sequences but may have different scores in each because of the differing failure modes leading to an accident. For example, a pipe may either plug or leak. A valve may leak, fail open, or fail closed. A complex piece of equipment such as a pump may have multiple different failure modes, each with a different likelihood, leading to several different accident sequences. The description of the accident sequence should clearly specify the conditions and failures that must occur for the undesired consequences to result.

Demand Rate: Demand rate refers to the frequency with which an IROFS having a specified probability of failure on demand is required to perform its safety function. The number of times an IROFS is required to work can have a significant effect on its likelihood of failure. For example, a particular administrative control may have a certain failure likelihood. However,

whether the accident sequence is "not unlikely," "unlikely," or "highly unlikely" will depend on the frequency with which the action is performed. If the action is required several hundred times a year, then occurrence of the initiating event will be significantly more likely than if the action is required once per year. Similarly, a passive control (such as the integrity of a storage container) may have a certain failure likelihood. However, if there are a thousand such containers in a storage array, then the likelihood that any one container will leak is much greater than if there is only one such container. Care must be taken to specify whether the initiating event is the leak of a particular container, or any one container, in the array.

Failure Rate: Failure rate refers to the frequency with which a continuously demanded item is observed to fail. In a qualitative method for likelihood evaluation, the failure rate is described in terms of qualitative descriptors (e.g., "several failures per year," "a few failures during facility lifetime," "no failures in 30 years for tens of similar IROFS in industry") used in the assignment

of qualitative likelihood scores (e.g., -1, -2, -3; A, B, C). This information is often not available with any precision, but when available, it should be used along with other qualitative information in the assignment of scores. This is because the failure rate represents an objective measure of the cumulative effect of all the reliability and availability qualities of the system. (See the discussion of qualitative and quantitative information below.)

This is not intended to be a comprehensive list of all facility- or process-specific factors that can affect the failure likelihood of individual IROFS.

Accident Sequences

Section 3.4.3.2(9) of this SRP states that there are other reliability and availability qualities that relate to characteristics of the entire system of IROFS credited in the accident sequence. This is because the accident sequence likelihood is not just a function of the likelihood of failure of the individual IROFS, but also of the relationship between the IROFS and between IROFS and initial conditions, bounding assumptions and design features.

Additional guidance on some of the specific reliability and availability qualities applicable to the accident sequence as a whole is provided below.

Defense in Depth: Defense in depth is the degree to which multiple IROFS or systems of IROFS must fail before the undesired consequences (e.g., criticality, chemical release) can result. IROFS that provide for defense in depth may be either independent or dependent, although IROFS should be independent whenever practical because of the possibility that the reliability of any single IROFS may not be as great as anticipated. This will make the results of the risk evaluation more tolerant of error. In addition, IROFS must be independent if the method for likelihood determination assumes independence (such as methods relying on summation of indices). IROFS are independent if there is no credible single event (common-mode failure) that can cause the safety function of each IROFS to fail. Multiple independent IROFS generally provide the highest level of risk reduction. The degrees of redundancy, independence, and diversity are important factors in determining the amount of risk reduction afforded by the system of IROFS.

Degree of Redundancy: Defense in depth is provided by specifying redundant IROFS that perform the same essential safety function. Redundant IROFS may be either diverse or

nondiverse; it is not necessary for them to consist of identical equipment or operator actions. However, when identical equipment or operator actions provide redundancy, it is important to ensure that all credible common-mode failures have been identified.

Degree of Independence: To qualify as independent, the failure of one IROFS should neither cause the failure nor increase the likelihood of failure of another IROFS. No single credible event should be able to defeat the system of IROFS such that an accident is possible. A systematic method of hazard identification should thus be used to provide a high degree of assurance that all credible failure mechanisms that could contribute to (i.e., by initiating or failing to prevent or mitigate) an accident have been identified. Methods commonly used for likelihood evaluation almost always assume that the chosen IROFS are independent. Examples of these methods include layer of protection analysis and the index method in Appendix A to this report. In a few cases, it may not be feasible to entirely eliminate the possibility of dependent failures. Methods that rely on independent IROFS should not be used to evaluate the likelihood of systems of IROFS with dependent failures. (Guidance applicable to the rare system with dependent failures is provided below.) If, however, the common-cause failure is sufficiently unlikely, it may be possible to treat IROFS as independent for purposes of the ISA and ISA

Summary, as discussed below. Because of the added requirement to meet the double-contingency principle, this approach will not be valid for criticality accident sequences when the requirements of 10 CFR 70.64(a)(9) apply.

Many factors can lead to IROFS not being independent, and these factors can have a significant effect on the likelihood of an accident sequence. A partial list of conditions that will almost always lead to two or more IROFS not being independent follows:

- The same individual performs administrative actions.
- Two different individuals perform administrative actions but use the same equipment and/or procedures.
- Two engineered controls share a common hardware component or common software.
- Two engineered controls measure the same physical variable using the same model or type of hardware.
- Two engineered controls rely on the same source of essential utilities (e.g., electricity, instrument air, compressed nitrogen, water).
- Two engineered controls are collocated such that credible internal or external events (e.g., structural failure, forklift impacts, fires, explosions, chemical releases) can cause both to fail.
- Administrative or engineered controls are susceptible to failure because of the presence of credible environmental conditions (e.g., two operator actions defeated by corrosive atmosphere, sensors rendered inoperable because of high temperature).

The presence of any of these conditions does not necessarily mean that the IROFS cannot be considered independent, but the applicant should provide additional justification demonstrating the lack of common-mode failure. The likelihood of such conditions in relation to the overall likelihood of an accident should be factored into the determination of the significance of the common-mode failure.

Diversity : Diversity is the degree to which IROFS that perform different safety functions provide defense in depth. This means that different types of failures must occur before an accident is

possible. Diverse controls may consist of controls on different parameters or different means of controlling the same parameter. In choosing redundant controls, preference should be given to diverse means of control, because they are generally less susceptible to common-mode failure than are nondiverse means. However, it is still necessary to consider all credible failure modes of the system when evaluating the overall likelihood of failure.

Vulnerability to Common-Cause Failure: Diverse means of control should be provided whenever practicable to minimize the potential for common-mode failure. For example, Chapter 5 of this SRP states that for criticality protection, a two-parameter control should be considered preferable to two controls on one parameter. Where a two-parameter control is not practicable, diverse means of controlling a single parameter should likewise be considered preferable to two redundant controls on that single parameter.

It is not always possible to provide absolute assurance that IROFS are perfectly independent. However, if the cumulative likelihood of all common-mode failures of a system of IROFS is significantly less than the independent failure of the system of IROFS, then the IROFS may be treated for all practical purposes as independent. Quantitatively, this means that the likelihood of the common-cause failure should be at least two orders of magnitude less than that of the independent failure of the system of IROFS. Qualitatively, this means that the likelihood of the common-cause failure should be sufficiently low that it does not change the score for the system of IROFS.

If credible common-mode failures cannot be neglected, as discussed above, then they must be considered in evaluating the overall accident sequence likelihood. A likelihood evaluation method (whether quantitative or qualitative) that correctly treats dependent failures should be used when such failures are present.

In general, the probability of failure of a system of two IROFS may be expressed as:

$$P(A,B) = Pifd(A,B) + Pdep(AB) = P(A)P(B) + Pdep(A,B)$$

That is, there is a component to the likelihood that is the independent failure of IROFS A and B and a component that represents the common-mode failure of IROFS A and B. Independent failure of the IROFS is represented by the product P(A)P(B). Therefore, the condition that the two IROFS be considered independent may be expressed as:

$$P(A,B) = P(A)P(B)$$

or equivalently

$$Pdep(AB) \ll P(A)P(B)$$

A variety of different methods may be used to treat dependent failures when the conditions above are not met. For example, in a quantitative method, the likelihood of the common-mode event may be estimated and factored into the above equation. In a qualitative scoring method, the likelihood score may be increased to reflect the existence of a common-mode failure. (In a qualitative scoring method similar to that employed in Appendix A to Chapter 3 of this SRP, summation of individual IROFS scores to determine the overall accident sequence score is permissible only if the IROFS are independent. Such a method assumes that independence

should be modified as needed to correctly treat common-mode failures.) In the layer of protection analysis method, only the independent IROFS are credited in evaluating the overall accident sequence likelihood. In a qualitative fault tree method, the common-mode failure may be included as an additional basic event in the fault tree. It is permissible then to treat the independent failure of the system of IROFS as one accident sequence and the dependent failure as another. The method used to treat dependent failures should be appropriately justified.

Qualitative criteria may be used to assess the effect of dependent failures on likelihood scores. The effect of qualitative performance-shaping factors should be considered in these criteria. For example, repeated failures of identical administrative IROFS (e.g., multiple batching, multiple valving, or spacing violations) should not be considered to be independent nor receive the same score without substantial justification, as discussed below. This is because the likelihood of. subsequent human failures increases once the initial failure has occurred. The set of factors

that could contribute to multiple administrative failures may include inadequate or out-of-date procedures, poor training, environmental distractions, and poor human factors design. For the same reason, the possibility of two different administrative failures by the same individual should be carefully considered for common-mode vulnerability. In assessing the vulnerability of these actions to common-mode failure, consideration may be given to any recovery factors that may be in place to interrupt the sequence of failures (e.g., supervisory checking, inspection, independent verification). Such recovery factors should be treated as measures that enhance the reliability of the administrative IROFS or ensure that repeated failures may be considered to be independent. In particular, independent verification of one administrative IROFS should not be used as a separate IROFS in the same accident sequence. For the same reasons as cited above, verification that an action has been performed correctly would be susceptible to the same factors that caused the initial failure. In addition, verification of an action is likely to be more cursory and, therefore, less reliable than performance of the original action. Moreover, in the event that the first action was performed correctly, the independent verification of that first action would not contribute to meeting the performance requirements, and therefore, the first action would constitute a sole IROFS. Thus, independent verification should be used only to increase the reliability of an IROFS and should not be treated as a separate IROFS nor credited with the same level of risk reduction.

In addition to the above, for criticality accident sequences required to comply with the double-contingency principle (see appendix 5-A of this SRP).

Use of Quantitative and Qualitative Information

Section 3.4.3.2(9) of this SRP acknowledges that a mix of quantitative and qualitative information is often available to an analyst performing an **ISA.** This SRP includes a list of some types of objective quantitative information and states that this information should be considered in evaluating likelihood, even in purely qualitative methods. The information listed includes (1) reports of equipment failures or procedural violations, (2) surveillance intervals, (3) functional testing intervals or audit frequencies, (4) time required to render the system safe, and (5) demand rates. In a purely qualitative method, such information, to the extent it is available, should be considered qualitatively. One example of this is using surveillance periods as part of the justification for qualitative duration indices (as in Appendix A to Chapter 3 of this SRP).

In using such objective data, facility-specific data are preferable to generic data, and process-specific data are preferable to facility-specific data because of the many environmental and other factors that can affect likelihood. For example, a manufacturer may have certified a particular pump with a given reliability rating, but the actual performance in process will depend on maintenance, electrical and mechanical loading, type of oil, ambient temperature, and vibration, among other factors. While more specific data are preferable, typically, the more specific the conditions, the fewer data are available. The amount and specificity of the data should be given appropriate weight in evaluating likelihood. For example, the use of generic failure data for a specific type of valve may be acceptable if an appropriately bounding value (i.e., the less conservative extreme of a range of values) is used. A less bounding value may be acceptable if information is available from the manufacturer on the specific model of valve. An even less bounding value may be acceptable if sufficient operating experience is available to support facility- or process-specific values. Sufficient margin to bound uncertainties in failure rates should be provided when relying on generic information.

Operating history may be credited in justifying likelihood scores for individual IROFS. Care must be taken that this credit is based on documented performance data and not anecdotal

evidence and that the operating history is applicable to the event being evaluated. For example, not having any criticality accidents in 30 years of operation would not be justification for a failure frequency for a particular component or initiating event (since the initiating event may have occurred several times during that time period without resulting in a criticality). It would also not be justification for a likelihood corresponding to a time between failures longer than 30 years. In addition, if significant facility changes occurred over the previous 30 years of operation, this information may not be meaningful. The limits and applicability of the operating data used to justify likelihood should be explained.

Especially for new processes or facilities, such objective quantitative data may not be available. Appropriate margin in plant operations and conservatism in likelihood scoring should be used and justified when such information is not available. Over the facility lifetime, however, information gained with regard to operational events and IROFS failures should be evaluated and fed back into the ISA process. This may be justification for reducing margins and conservatism over the facility lifetime.

Graded Approach to Integrated Safety Analysis

The performance requirements of 10 CFR 70.61(b) and (c) establish an acceptable level of risk, in that high-consequence events must be made "highly unlikely" and intermediate-consequence events must be made "unlikely." In addition, 10 CFR 70.65(b)(4) requires that an applicant's ISA Summary contain a demonstration of compliance with the performance requirements of 10 CFR 70.61. The means and the level of effort required to demonstrate compliance with 10 CFR 70.61 depend on the amount of risk reduction needed to meet the likelihood thresholds in that regulation. For example, a facility that obviously has inherently low risk (even before the performance of the ISA) requires less effort to demonstrate compliance than an inherently higher risk facility. Examples would include facilities with small mass or very low enrichment of special nuclear material, low chemical inventories, or insignificant combustible loading. Thus, the ISA methods used may be graded commensurate with the risk of the facility.

The facility and process characteristics that determine inherent risk should be identified as initial conditions and/or bounding assumptions and/or design features and appropriately identified and maintained to ensure that they will be present over the lifetime of the facility, if credit is taken for

them in meeting the performance requirements. For example, a possession limit on the maximum enrichment or amount of special nuclear material at the facility may be credited in ensuring low risk of criticality, because the license sets an explicit limit. Chemical inventories may be likewise credited, provided that they are limited by license or the maximum inventory is identified as important to safety and rigorously controlled. ISA methods may be graded commensurate with the amount of risk reduction required once these factors have been explicitly identified and maintained.

The following are examples of aspects of the ISA process that may be graded commensurate with risk:

- In the selection of the hazard identification method, the what-if or what-if/checklist method would be more suitable for low-risk, simple operations; hazardous operations, fault tree, and other sophisticated methods may be appropriate for more complex or higher risk operations.

- In the evaluation of the type, number, and robustness of IROFS, lower risk facilities will not require the same level of control.

- In the application of management measures, lower risk facilities will not require measures as stringent as those for higher risk facilities.

- In the evaluation of likelihood, the technical justification required to support a high degree of risk reduction is much greater than that required to support a low or moderate degree of risk reduction. Methods used to support a high degree of risk reduction should be more sophisticated, and warrant greater regulatory scrutiny, than methods used to support a lower degree of risk reduction.

In addition to the inherent risk of the facility or process, the amount of conservatism may be considered in grading ISA methods. For example, if a very conservative likelihood is assumed for all IROFS failures, then the rigor and level of detail in describing the IROFS, considering all reliability and availability qualities and treating dependent failures, would not have to be at the same level as in a facility taking more realistic credit for IROFS failures. The grading of ISA methods necessitates that the applicant demonstrate (1) that the risk is inherently low and will be maintained over the lifetime of the facility, or (2) that there is a consistent and dependable amount of conservatism in ISA methods that offsets the uncertainty arising from lack of rigor.

Regulatory Basis

The risk of each credible high-consequence event must be limited. Engineered controls, administrative controls, or both shall be applied to the extent needed to reduce the likelihood of occurrence of the event so that, upon implementation of such controls, the event is highly unlikely or its consequences are less severe than those described in 10 CFR 70.61(b)(1-4).

The risk of each credible intermediate-consequence event must be limited. Engineered controls, administrative controls, or both shall be applied to the extent needed so that upon implementation of such controls, the event is unlikely or its consequences are less than those described in 10 CFR 70.61(c)(1-4).

Each licensee or applicant shall conduct and maintain an ISA that is of appropriate detail for the complexity of the process and that identifies "the consequences and likelihood of occurrence of each potential accident sequence.. .and the methods used to determine the consequences and likelihoods," as stated in 10 CFR 70.62(c)(1)(v).

The ISA Summary must contain "information that demonstrates the licensee's compliance with the performance requirements of Section 70.61 ," as stated in 10 CFR 70.65(b)(4).

The ISA Summary must also include the definitions of "unlikely," "highly unlikely," and "credible" as used in the evaluations of the ISA, as stated in 10 CFR 70.65(b)(9).

Technical Review Guidance

The reviewer should use the information contained in this appendix, as applicable, to evaluate an applicant's or a licensee's qualitative methods of likelihood evaluation, commensurate with the level of risk reduction required to comply with the performance requirements of 10 CFR 70.61. If the applicant is using the index method defined in Appendix **A** to Chapter 3 of this SRP, the reviewer should use the guidance in Appendix A to evaluate the adequacy of the applicant's ISA Summary. The purpose of the ISA Summary review is not to verify the

correctness of the likelihood scores for every single accident sequence, but to verify that the applicant has an acceptable methodology that contributes to reasonable assurance of maintaining an adequate safety basis over the facility lifetime, by ensuring that the methodology results in assignment of appropriate likelihoods. Thus, the reviewer should primarily determine whether there is a justifiable basis for the scores, and whether there is reasonable assurance that this basis will be maintained over the facility lifetime, assuming the application of appropriate management measures.

The applicant's qualitative method for likelihood evaluation should be acceptable if the following are true:

- The definitions of likelihood are clear, are based on objective criteria, and can consistently distinguish events in different likelihood categories.
- The methods for likelihood evaluation are consistent with the likelihood definitions and the process being evaluated (e.g., the methods correctly treat initiating events, ~~and~~ initial conditions, bounding assumptions, and design features, subsequent failures, and dependent failures).
- The methods for likelihood evaluation appropriately consider all availability and reliability
- qualities of individual IROFS and the interdependencies between them in assigning qualitative likelihood scores.

The ISA Summary describes initiating events, initial conditions, and subsequent IROFS failures in detail sufficient to demonstrate that the performance requirements will be met and maintained.

Recommendations

This guidance should be used to supplement Chapter 3 and Appendix **A** to this SRP.

References

U.S. Code of Federal Regulations, Title 10, "Energy," Part 70, "Domestic Licensing of Special Nuclear Material."

U.S. Nuclear Regulatory Commission, "Standard Review Plan for the Review of an Application for a Mixed Oxide (MOX) Fuel Fabrication Facility," NUREG-1718, August 2000.

APPENDIX C
INITIATING EVENT FREQUENCY

Purpose

This appendix addresses the measures needed to ensure the validity and maintenance of the initiating event frequencies (IEFs) used to demonstrate compliance with Title 10 of the Code *of Federal Regulations (10* CFR) 70.61, "Performance Requirements."

Introduction

The purpose of this appendix is to clarify the use of IEFs for demonstrating compliance with the performance requirements of 10 CFR 70.61. NUREG-1718, "Standard Review Plan for the Review of an Application for a Mixed Oxide (MOX) Fuel Fabrication Facility," issued August 2000, and this Standard Review Plan (SRP) provide methods for reviewing integrated safety analyses (ISAs) by employing a semi-quantitative risk index method. While one of these methods is described below to illustrate the use of IEFs, applicants and licensees may use other methods that would produce similar results. No particular method is explicitly mandated, and sequences that are risk significant or marginally acceptable are candidates for more detailed evaluation by the applicant or licensee and reviewer.

Discussion

Each licensee or applicant is required to perform an ISA to identify all credible high consequence and intermediate-consequence events. The risk of each such credible event is to be limited through the use of appropriate engineered and/or administrative controls to meet the performance requirements of 10 CFR 70.61. Such a control is referred to as an item relied on for safety (IROFS). In turn, a safety program must be established and maintained to ensure that each IROFS is available and reliable to perform its intended function when needed. The safety program may be graded such that the management measures applied are graded commensurate with the reduction of risk attributable to that item. In addition, a configuration management system must be established pursuant to 10 CFR 70.72, "Facility Changes and Change Process," to evaluate changes and to ensure, in part, that the IROFS are not removed without at least equivalent replacement of the safety function.

The risk of each credible event is determined by cross-referencing the severity of the consequence of the unmitigated accident sequence with the likelihood of occurrence in a risk matrix with risk index values. The likelihood of occurrence risk index values can be determined by considering the criteria in Tables A-9 through **A-1** 1 in Appendix A to Chapter 3 of this SRP. Accident sequences result from initiating events that are followed by the failure of one or more IROFS. Initiating events can be (1) an external event such as a hurricane or earthquake, (2) a facility event external to the process being analyzed (e.g., fires, explosions, failures of other equipment, flooding from facility water sources), (3) deviations from normal operations of the process (credible abnormal events), or (4) failures of an IROFS in the process. (Appendix D to Chapter 3 offers additional guidance regarding initiating probabilities from natural phenomena hazards.)

An initiating event does not have to be an IROFS failure. An item becomes an IROFS only if the

ISA credits it for mitigation or prevention per the definition in 10 CFR 70.4, "Definitions." If an item whose failure initiates an event has strictly an operational function, it does not have to be an IROFS. This applies to external events and can apply to internal events. If the item whose failure initiates an event has solely a safety function that is ~~credited in the ISA~~required to meet the performance requirements of 10CFR70.61, then it should be an IROFS. If the item has both an operational and a safety function, the safety function should make it an IROFS (for its ISA-credited safety features only).

IEFs can play a significant role in determining whether the performance requirements of 10 CFR 70.61 are met for a particular accident sequence. Whether an initiating event results from an IROFS or a non-IROFS failure, licensees should take appropriate action to ensure that any change to the basis for assigning an **IEF** value to that event is evaluated on a continuing basis to ensure continued compliance with the performance requirements. For example, a non-IROFS component may not be subject to the same quality assurance (QA) program controls and other management measures that an IROFS would receive (i.e., surveillance, testing, procurement). However, appropriate management controls should be considered, in a graded manner, to provide assurance that performance requirements are met over time. The ability to identify a non-IROFS component failure, similar to that for IROFS, may be needed to provide feedback on failure rates and IEFs to the ISA process. Changes to the **IEF** values may result from changes to a component's design, procurement, operation, or maintenance history, as well as new or increased external plant hazards, and should be considered in a graded approach.

Regulatory Basis

This guidance relies on the following regulatory bases:
* 10 CFR 70.61
* 10 CFR 70.62, "Safety Program and Integrated Safety Analysis"
* 10 CFR 70.65, "Additional Content of Applications"
* 10 CFR 70.72, "Facility Changes and Change Process"

Applicability

This guidance is for use in those cases where an applicant or licensee chooses to use an IROFS or non-IROFS failure IEF for risk determination.

Technical Review Guidance

1. Initiatinq Event Frequency and Identification of an IROFS

Example
A licensee uses a heater/blower unit to heat a uranium hexafluoride (UF_6) cylinder in a hot box to liquefy the contents before sampling. The unmitigated accident sequence involves the failure of the controller for the heater/blower resulting in overheating of the cylinder. This results in the cylinder becoming overpressurized and rupturing, which releases the UF_6 to the surrounding process area. Analysis of such a release indicates that it would exceed the performance requirements of 10 CFR 70.61. The licensee has two basic choices: (1) assume that the initiating event probability equals 1 and provide

an appropriate level of mitigation or prevention solely through one or more IROFS or (2) assign a value to the initiating event (blower/heater controller failure) and provide one or more preventive or mitigative IROFS to bring the accident sequence risk within the performance requirements.

If the licensee chooses the second option and assigns an appropriate value to the IEF, the indices of Table A-9 in Appendix A to Chapter 3 of this SRP may be used. The controller for the heater/blower unit would be assigned an appropriate frequency index number. The licensee would then analyze the accident sequence and determine whether additional IROFS are necessary to meet the performance requirements. There are now two variables that feed into the risk determination: one or more IROFS controllers for the heater/blower unit in a manner that changes the licensee's previous determination of compliance with the performance requirements must be evaluated per 10 CFR 70.72(a).

2. Initiating Event Frequency Index Use

Indices may be used to determine the overall likelihood of an accident sequence. Table A-9 of Appendix A to Chapter 3 of this SRP identifies frequency index numbers based on specified evidence. The evidence used by applicants and licensees should be supportable and documented in the ISA Summary as required by 10 CFR 70.65(b)(4). The evidence cited in the ISA documentation should not be limited to anecdotal accounts and must demonstrate compliance with the definitions of "unlikely," "highly unlikely," and "credible" as required by 10 CFR 70.65(b)(9). The rigor and specificity of the documented evidence should be commensurate with the item's importance to safety, and the data should support the frequency chosen (e.g., data from 30 years of plant operating experience based on a single component typically could not be expected to support a 10-2 failure probability).

An item's failure rate should be determined from actual data for that specific component or safety function in the current system design under the current environmental conditions. When specific failure data are limited or not available, the applicant or licensee may use more "generic" data with appropriate substantiation. However, when less specific failure data are available, appropriate conservatism should be exercised in assigning frequency indices. The footnote to Table A-9 that states "Indices less than (more negative than) -1 should not be assigned to IROFS unless the configuration management, auditing, and other management measures are of high quality, because without these measures, the IROFS may be changed or not maintained" should also be applied to non-IROFS IEFs. In this case, appropriate management controls should be provided to ensure that any changes to the evidence supporting **IEF** indices will be identified and promptly evaluated to ensure that the performance requirements of 10 CFR 70.61 are met. A graded approach may be used in applying management controls based on the IEF values; however, the ISA Summary should explain how this will be done.

The licensee or applicant should periodically evaluate possible changes to IEFs, failure rates, and the assumptions they are based on to ensure that the ISA process has accounted for any change to an IEF. Over time, an IEF may change because of component aging or deterioration. Maintenance and performance experience should be fed back into the IEF evaluation. **IEF** changes could involve, for example, the introduction of new effects or hazards from nearby processes or new materials or

changes in design, maintenance, or operation activities. The applicant or licensee should establish management measures, which may be graded, to periodically confirm that the ISA assumptions have not changed. For example, an applicant or licensee may choose to verify that there have been no changes to hazards from maintenance activities during a certain period of time based on an appropriate documented technical review or audit under the QA program.

Whatever strategy the applicant or licensee chooses should result in timely identification and periodic evaluation of failure rates, followed by a prompt evaluation of the failure rate change on the ISA assumptions. This can be accomplished in accordance with the corrective maintenance program and/or the QA problem identification and corrective action system.

Indices particularly relied on (i.e., less than -1) for overall likelihood will be examined during the ISA review process.

3. External Initiating Event Frequencies

The applicant or licensee should periodically evaluate possible changes to nonnatural phenomena external events to ensure that the ISA process has accounted for any change to an IEF. Such changes could involve, for example, the introduction of new hazards from an adjoining industrial site or changes in adjoining transportation activities. The applicant or licensee should establish management measures, which may be graded, to periodically confirm that the ISA assumptions have not changed. For example, an applicant or licensee may choose to verify that external hazards have not changed based on a 2- to 3-year review under the QA program.

4. Assurance

The safety program required by 10 CFR 70.62(a) should have provisions for implementing the appropriate management controls to maintain the validity of the IEFs. Consideration should also be given to commitments in the QA program or a specific license condition.

References

U.S. Code of Federal Regulations, Chapter I, Title 10, "Energy," Part 70, "Domestic Licensing of Special Nuclear Material."
U.S. Nuclear Regulatory Commission, "Standard Review Plan for the Review of an Application for a Mixed Oxide (MOX) Fuel Fabrication Facility," NUREG-1718, August 2000.