FCSS Interim Staff Guidance-01, Revision 0
Qualitative Criteria for Evaluation of Likelihood

Prepared by
Division of Fuel Cycle Safety and Safeguards
Office of Nuclear Material Safety and Safeguards

Issue

Use of qualitative criteria in methods for evaluation of likelihood for demonstrating compliance with the performance requirements of Title 10 of the Code of Federal Regulations (10 CFR), Section 70.61.

Introduction

Section 70.61(b) of 10 CFR 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. Section 70.61(c) of 10 CFR 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. Part 70 of 10 CFR does not define the terms “highly unlikely,” “unlikely,” and “credible,” but instead states that definitions of these terms must be included in the applicant’s Integrated Safety Analysis (ISA) Summary.

As stated in NUREG-1520, “Standard Review Plan for the Review of a License Application for a Fuel Cycle Facility,” Section 3.4.3.2(9), 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 (semi-quantitative methods) may rely on a mixture of qualitative and quantitative definitions, methods, and information. NUREG-1520 provided general guidance on the use of qualitative methods for evaluation of likelihood. However, the NRC’s review of recently submitted ISA Summaries has revealed a lack of common understanding as to what constitutes an acceptable qualitative method.

The purpose of this Interim Staff Guidance (ISG), therefore, is to provide additional guidance and clarify existing guidance 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. These accident sequences may be initiated by either external events or internal events (which may or may not be IROFS failures). Additional guidance on the use of initiating events which are natural phenomena is provided in ISG-08, “Natural Phenomena Hazards.” Additional guidance on the use of initiating events which are internal to the facility is provided in ISG-09, “Initiating Event Frequency.” That guidance may be used together with the guidance in this ISG as an acceptable qualitative method for likelihood evaluation.

Discussion

Definitions of Likelihood

Section 70.65(b)(9) of 10 CFR requires that the ISA Summary must contain a description of the definitions of unlikely, highly unlikely, and credible. NUREG-1520, Section 3.4.3.2(9), states that qualitative definitions of likelihood are acceptable if they meet two conditions: (a) they are reasonably clear and based on objective criteria; and (b) 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 so 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 the performance requirements are met.

NUREG-1520 states that "objective criteria" means the method relies on specific identifiable characteristics of a process design, rather than subjective judgements 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 IROFS (e.g., whether the IROFS are independent), the characteristics of the process design which the method should rely on are the specific identifiable characteristics of the initiating event, IROFS failures, and other process 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. These features are described in detail in the following sections. It is important that any features of the process or equipment necessary to meet the performance requirements is recognized as important to safety and appropriately maintained through the use of management measures.

Examples of acceptable qualitative definitions of likelihood are the second and third definition of "not credible" in NUREG-1520, Section 3.4.3.2(9):

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

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

> 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 what is meant by being present to

an appropriate degree. Other definitions are acceptable provided they meet the two criteria specified above and the system features ensuring the likelihood are appropriately maintained.

Evaluation of Likelihood

Accident sequences, in general, consist of an initiating event followed by the occurrence of 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: (a) are reasonably clear and based on objective criteria, and (b) 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 NUREG-1520 as the *reliability and availability qualities* of IROFS or systems of IROFS.

Initiating Events/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 man-made event), an internal event other than an IROFS failure, or an IROFS failure. Natural phenomena events may include heavy rains, winds, flooding, earthquakes, fires, etc. External man-made events may include impacts from nearby facilities, aircraft or vehicle crashes, fires, loss of offsite utilities, etc. Internal events other than IROFS failures may include spills, non-IROFS equipment failure, process deviations, industrial accidents, loss of onsite utilities, etc. 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 non-numerical (e.g., A, B, C, D) form but is still qualitative if based on qualitative criteria.

The likelihood of external initiating events (by definition outside the control of the facility) does not rely on any design features of the facility or process, and are 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 having 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 “1000-year earthquake,” or may include other qualitative criteria capable of being correlated to a frequency, such as “design basis earthquake,” or “exceeds the mean annual rainfall by a factor of x.” By contrast, quantitative or semi-quantitative methods may include quantitative descriptions of frequency such as “having a frequency less than 10^{-2}/yr.” Because these are beyond human control, there are no features that have to be maintained to ensure the continued validity of the assigned likelihood. However, it may be necessary to periodically reexamine the basis for these likelihoods if it is reasonably expected the likelihood could change (e.g., following construction of a new railroad spur next to the facility). ISG-08, “Natural Phenomena Hazards,” contains additional guidance applicable to initiating events which 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 upon objective evidence of their frequency of occurrence or upon 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 this 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 that can affect the event likelihood (reliability and availability qualities) are recognized as such and appropriately maintained. ISG-09, "Initiating Event Frequency," contains additional guidance applicable to internal initiating events other than IROFS failures.

Similarly, the likelihood of internal initiating events which are IROFS failures also depends on specific, identifiable characteristics of the facility or process design. Scores may be assigned to such events based either upon objective evidence of their frequency of occurrence or upon 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 appropriately maintained. Guidance on specific reliability and availability qualities associated with individual IROFS is provided below.

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 must be identified, and, if susceptible to change over the lifetime of the facility (such as through process deviations or facility changes) must be appropriately maintained. For example, the maximum throughput or inventory in a process may change and thus measures should be put in place to maintain it if relied on to meet the performance requirements, whereas the flow of gravity or maximum density may not require specific controls.

Individual IROFS

NUREG-1520, Section 3.4.3.2(9), states that the reliability and availability qualities of individual IROFS include: (a) safety margin in the controlled parameter, (b) the type of IROFS (passive or active engineered, simple or enhanced administrative), (c) the type and safety grading of any management measures, (d) whether the system is fail-safe, failure is self-announcing, or the IROFS is subject to periodic surveillance, (e) failure modes, (f) demand rate, and (g) failure rate. It is very important that any qualitative (or quantitative) method of likelihood evaluation consider all applicable IROFS attributes that could affect its reliability and availability, 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 considerations that may be present should be appropriately taken into account. For example, environmental conditions may have a significant effect on IROFS reliability (e.g., extreme temperatures and

pressures, corrosive atmosphere, excessive vibration) and should be appropriately taken into account.

The level of detail in 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. Section 70.65(b)(6) of 10 CFR 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: (1) the boundary of an enhanced administrative IROFS includes all instrumentation (sensors, annunciators, circuitry, any controls activated by the operator, etc.) relied on to trigger the operator action; (2) the boundary of a simple administrative control includes the equipment necessary to correctly perform the action; and (3) 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* is taken to mean 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 being unlikely or highly unlikely based on safety margin, the margin should be several times larger than the expected process variation or uncertainty. Similarly, the fact that the margin is much greater than the change in the parameter resulting from the worst-case credible upset could be credited for ensuring the event is unlikely or highly unlikely.

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

Type of Control: Passive engineered controls are generally considered to be preferable to active engineered controls, active engineered controls to enhanced administrative controls, and enhanced administrative controls 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/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 in quantitative fashion in the ISA Summary. For example, it may be sufficient to specify that maintenance will be performed on a frequency and in a manner consistent with the manufacturer's recommendations, in order to take credit for generic failure rates for that piece of equipment. Functional testing should be conducted in a manner that ensures that everything within the IROFS boundary is functioning 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/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 only considered to fail when it fails to perform its intended safety function. Thus, a valve which is an IROFS is not considered to fail in the context of the accident sequence (i.e., contribute to the progression of an accident sequence) as long as it 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 which 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 essentially immediately corrected. 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 due to 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 what the conditions and failures are necessary to result in the undesired consequences.

Demand Rate: Demand rate refers to the frequency with which an IROFS having a specified probability of failure on demand (PFOD) 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 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 where 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

NUREG-1520, Section 3.4.3.2(9), 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 of the relationship between the IROFS.

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 which 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 or risk reduction. The degree 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 which perform the same essential safety function. Redundant IROFS may be either diverse or non-diverse; it is not necessary for them to consist of identical equipment or operator actions. However, when redundancy is provided by identical equipment or operator actions, 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., initiate or fail 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 (LOPA) and the index method of Appendix A of NUREG-1520. In a small number of 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. Note that 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.

There are numerous factors that could lead to IROFS not being independent, and the presence of 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:

- Administrative actions are performed by the same individual.
- Administrative actions are performed by two different individuals but using 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 susceptible to failure due to presence of credible environmental conditions (e.g., two operator actions defeated by corrosive atmosphere, sensors rendered inoperable due to high-temperature).

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

Diversity: Diversity is the degree to which defense-in-depth is provided by IROFS which perform different safety functions, such that different types of failures are required 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 non-diverse. 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, NUREG-1520, Section 5.4.3.4.4(7)(a), 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 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 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:

$$P(A,B) = P_{ind}(A,B) + P_{dep}(A,B) = P(A)P(B) + P_{dep}(A,B)$$

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:

$$P(A,B) \approx P(A)P(B)$$

or equivalently

$$P_{dep}(A,B) << P(A)P(B)$$

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 of NUREG-1520, summation of individual IROFS scores to determine the overall accident sequence score is only permissible if the IROFS are independent. Such a method assuming independence should be modified as needed to correctly treat common-mode failures.) In the LOPA 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 employed in assessing the effect of dependent failures on likelihood scores. The effect of qualitative performance shaping factors should be taken into account 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 there is an increased likelihood of subsequent human failures 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, poor human factors design, etc. Likewise, occurrence of two different administrative failures by the same individual should be carefully considered for common-mode vulnerability for the same reason. 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., supervisor 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 those 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 only be used 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 (DCP), the guidance of ISG-03, "Nuclear Criticality Safety Performance Requirements and Double Contingency Principle," is applicable.

Use of Quantitative and Qualitative Information

NUREG-1520, Section 3.4.3.2(9), acknowledges that often there is a mix of quantitative and qualitative information available to an analyst performing an ISA. NUREG-1520 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 taken into account in a qualitative way. One example of this is using surveillance periods as part of the justification for qualitative duration indices (as in Appendix A of NUREG-1520).

In making use of such objective data, the use of facility-specific data is preferable to generic data, and process-specific data is 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, etc. While more specific data is preferable, it is acknowledged that typically the more specific the conditions, the less data is 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.

It is acknowledged, 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 ISA

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 depends on the amount of risk-reduction that is needed to meet the likelihood thresholds in 10 CFR 70.61. For example, a facility that has obviously inherently low risk (even before the performance of the ISA) require 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 (SNM), 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 assumptions and appropriately identified and maintained to ensure they will be present over the lifetime of the facility, if credit is taken for these in meeting the performance requirements. For example, a possession limit on the maximum enrichment or amount of SNM at the facility may be credited in ensuring low risk of criticality, because this is explicitly limited in the license. 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.

Several examples of aspects of the ISA process which may be graded commensurate with risk include:

- Selection of the hazard identification method (the What-If or What-If/Checklist method would be more suitable for low-risk, simple operations; HazOp, Fault Tree, and other sophisticated methods may be appropriate for more complex or higher-risk operations).

- Type, number, and robustness of IROFS (lower-risk facilities will not require the same level of control).

- Application of management measures (lower-risk facilities will not require as stringent management measures).

- 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 due to 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 in paragraphs (b)(1)-(4) of 10 CFR 70.61(b).

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 in paragraphs (c)(1)-(4) of 10 CFR 70.61(c).

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

The integrated safety analysis summary must contain "information that demonstrates the licensee's compliance with the performance requirements of Section 70.61..." as referenced in 10 CFR 70.65(b)(4).

"A description of the definitions of unlikely, highly unlikely, and credible as used in the evaluations in the integrated safety analysis," can be found in 10 CFR 70.65(b)(9).

Technical Review Guidance

The reviewer should use the information contained in this ISG, as applicable, to evaluate an applicant's or 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 of NUREG-1520, the reviewer should use the guidance in Appendix A of this ISG 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 whether the applicant has an acceptable methodology such that there is reasonable assurance of maintaining an adequate safety basis over the facility lifetime, by ensuring that the methodology results in assignment of appropriate likelihoods. As such, 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 that appropriate management measures are applied.

The applicant's qualitative method for likelihood evaluation should be acceptable if:

- The definitions of likelihood are clear and 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., correctly treat initiating events and initial conditions, subsequent failures, and dependent failures).

- The methods for likelihood evaluation appropriately take all availability and reliability qualities of individual IROFS and the interdependencies between them into account in assigning qualitative likelihood scores.

- Initiating events, initial conditions, and subsequent IROFS failures are described in sufficient detail in the ISA Summary to demonstrate that the performance requirements will be met and maintained.

Recommendations

This guidance should be used to supplement NUREG-1520, Chapter 3, "Integrated Safety Analysis (ISA) and ISA Summary," and Appendix A, "Example Procedure for Accident Sequence Evaluation."

This guidance should be used to supplement NUREG-1718, Chapter 5, "Integrated Safety Analysis (ISA)," and Appendix A, "Example Procedure for Risk Evaluation."

References

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

U.S. Nuclear Regulatory Commission (U.S.) (NRC). NUREG-1520, "Standard Review Plan for the Review of a License Application for a Fuel Cycle Facility." NRC: Washington, D.C. March 2002.

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

Approved: _____**/RA/**_____ Date: _June 9, 2005___
Robert C. Pierson, Director
Division of Fuel Cycle Safety
and Safeguards, NMSS

Appendix A

Use of NUREG-1520, Appendix A Methodology

Introduction

The purpose of this appendix is to provide additional clarification on the proper use of the semi-quantitative index method as described in Appendix A of NUREG-1520, "Standard Review Plan for the Review of a License Application for a Fuel Cycle Facility." Several licensees and applicants have made use of the index method of Appendix A (or a variation thereof) in performing their integrated safety analyses (ISAs). The U.S. Nuclear Regulatory Commission (NRC) review of these licensees' and applicants' ISA Summaries has highlighted a need for additional guidance on the use of this method. Because of its widespread use and a lack of common understanding about the use of this method, guidance on the index method is appropriate.

As stated in the introduction to Appendix A of NUREG-1520, the index method is but one method of likelihood evaluation. The index method is not strictly a *qualitative* method, but is a *semi-quantitative* method that considers both qualitative and quantitative information (if it is available and applicable). In this method, the definition of likelihood terms (i.e., not unlikely, unlikely, and highly unlikely) is expressed quantitatively (more than 10^{-4} per event per-year, between 10^{-4} and 10^{-5} per-event per-year, and less than 10^{-5} per-event per-year respectively). Whereas a purely qualitative method would use purely qualitative definitions of likelihood and qualitative methods of evaluating likelihood, much of the quantitative discussion in this appendix would not apply. However, this method is illustrative of the thought processes that should be used in even a purely qualitative method.

The index method is one acceptable method of demonstrating compliance with the performance requirements. However, taking credit for using this method requires that the applicant follow all of the guidance contained in Appendix A of NUREG-1520. Otherwise, additional justification should be provided.

Likelihood Definitions

The likelihood definitions in Table A-6 of NUREG-1520 are, as stated above, described in quantitative terms (e.g., highly unlikely is defined as less than 10^{-5} per-event per-year). The footnote to Table A-6 states, however, that these are based on approximate order-of-magnitude ranges. Therefore, they should not be regarded as strict numerical limits, but as indicative of the approximate order of magnitude of likelihood. Any definition of likelihood should be stated on a per-event basis.

Likelihood Evaluation Method

The likelihood evaluation method used should be consistent with the likelihood definitions, such that the qualitative score assigned can be compared to the likelihood definitions. In the index method, the likelihood index for the accident sequence must be no greater than -5 to meet the

definition of highly unlikely, and must be no greater than -4 to meet the definition of unlikely. The likelihood index for the accident sequence is determined by summing likelihood indices for the initiating event and subsequent items relied on for safety (IROFS) failures. Criteria for the assignment of the likelihood indices are contained in Tables A-9, A-10, and A-11 of NUREG-1520.

Appendix A of NUREG-1520 distinguishes between two different kinds of events that can be combined to form the accident sequences in the ISA Summary. The two basic kinds of events are: (1) events that are characterized by a frequency of occurrence, and (2) events that are characterized by a probability of failure on demand (PFOD). In the index method of Appendix A, the category to which an event belongs determines how it is scored by means of either Table A-9 or A-10, as explained below.

Events characterized by a frequency of occurrence (f-type events) can include external events, internal events that are not IROFS failures, or IROFS failures. Examples of external and internal events that are not IROFS failures are provided in the text of the ISG. IROFS failures that are characterized by a frequency of occurrence are those that are required to be continuously present, rather than those which are required to perform a safety function only when certain conditions are present. Examples may include favorable geometry equipment or an active engineered device monitoring a continuous process.

Events characterized by a probability of failure on demand (p-type events) typically include IROFS which are not required to be continuously present, but which must perform a safety function on demand (subsequent to some process deviation or failure). Examples may include active interlocks that perform some protective function when system parameters exceed preset limits, administrative controls required in response to process deviations, or certain administrative controls in batch processes. These are usually part of the subsequent failures following the initiating event but may, on occasion, be present as part of the initiating event.

Accident sequences may in general be composed of a large number of individual events. In general, accident sequences consist of an initiating event followed by the failure of one or more IROFS. Because overall accident sequence likelihood must be consistent with the likelihood categories, it must have the same dimensional units as those in the likelihood definitions (i.e., probability per-event per-year). Even though qualitative indices are used instead of quantitative probabilities, this requirement imposes constraints on the ways in which individual indices may be combined.

For simplicity, only two-event sequences (in which the events are independent) are considered below. Based on the two basic kinds of events, there are four basic types of two-event accident sequences, as follows:

<u>F-Type Initiating Event with Subsequent P-Type IROFS Failure</u>

Using the index method of Appendix A of NUREG-1520, a failure frequency index may be applied to the initiating event using the criteria in Table A-9, and a failure probability index may be applied to the subsequent IROFS failure using the criteria in Table A-10. The overall likelihood index for the accident sequence is the sum of the likelihood indices for the two events. This is because the IROFS is assumed to be demanded every time the initiating event occurs.

Mathematically, this results in an accident sequence likelihood index corresponding to an accident sequence likelihood with the correct dimensional units:

Accident sequence likelihood (yr^{-1}) = initiating event frequency (yr^{-1}) × PFOD

Accident sequence index = initiating event index + subsequent failure index

An example of this type of accident sequence is a criticality sequence consisting of a loss of concentration control in a continuous solution processing operation, followed by failure of an in-line concentration monitor that closes an isolation valve on a transfer line upon detection of highly concentrated solution.

F-Type Initiating Event with Subsequent F-Type IROFS Failure

Using the index method of Appendix A of NUREG-1520, a failure frequency index may be applied to both the initiating event and the subsequent IROFS failure using the criteria in Table A-9. The overall likelihood index for the accident sequence is the sum of the individual likelihood indices for the two events and a *duration index* for the initiating event. This is because the probability of the second event occurring concurrent with the first event is dependent on the time during which the conditions caused by the first event persist. In order for the accident sequence likelihood to have the correct units (yr^{-1}), the duration of failure for the first event must be taken into account.

Mathematically, this results in an accident sequence likelihood index corresponding to an accident sequence likelihood with the correct dimensional units:

Accident sequence likelihood (yr^{-1}) = initiating event frequency (yr^{-1}) × initiating event duration (yr) × subsequent failure frequency (yr^{-1})

Accident sequence index = initiating event index + initiating event duration index + subsequent failure index

An example of this type of accident sequence is a criticality sequence consisting of a loss of geometry control followed by a loss of moderation control due to unrelated sprinkler activation before geometry control can be restored.

P-Type Initiating Event with Subsequent P-Type IROFS Failure

Using the index method of Appendix A of NUREG-1520, a failure probability index may be applied to both the initiating event and the subsequent IROFS failure using the criteria in Table A-10. The overall likelihood index for the accident sequence is the sum of the individual likelihood indices for the two events, which includes consideration of the *demand rate* associated with the initiating event. This is because the total failure frequency for the initiating event depends on the frequency with which the demand occurs as well as the associated PFOD. The subsequent IROFS is assumed to be demanded every time the initiating event occurs. In order for the accident sequence likelihood to have the correct units (yr^{-1}), the demand rate of the first event must be taken into account.

Mathematically, this results in an accident sequence likelihood index corresponding to an accident sequence likelihood with the correct dimensional units:

> Accident sequence likelihood (yr^{-1}) = initiating event demand rate (yr^{-1}) × initiating event PFOD × subsequent event PFOD
>
> Accident sequence index = initiating event index (including demand rate) + subsequent failure index

An example of this type of accident sequence is a criticality sequence consisting of the failure of an operator to sample solution prior to transfer in a batch operation, followed by failure of an in-line concentration monitor as discussed previously.

P-Type Initiating Event with Subsequent F-Type IROFS Failure

Using the index method of Appendix A of NUREG-1520, a failure probability index may be applied to the initiating event using the criteria in Table A-10. A failure frequency index may be applied to the subsequent IROFS failure using the criteria in Table A-9. The overall likelihood index for the accident sequence is the sum of likelihood indices for the two events, which includes consideration of the *demand rate* associated with the initiating event, and a *duration index* for the initiating event. This is because the failure frequency for the initiating event depends on the frequency with which the demand occurs as well as the associated PFOD. The probability of the second event occurring concurrent with the first event is dependent on the time during which the conditions caused by the first event persist. In order for the accident sequence likelihood to have the correct units (yr^{-1}), both the duration of failure for the first event and its demand rate must be taken into account.

Mathematically, this results in an accident sequence likelihood index corresponding to an accident sequence likelihood with the correct dimensional units:

> Accident sequence likelihood (yr^{-1}) = initiating event demand rate (yr^{-1}) × initiating event PFOD × initiating event duration (yr) × subsequent failure frequency (yr^{-1})
>
> Accident sequence index = initiating event index (including demand rate) + failure duration index + subsequent failure index

An example of this type of accident sequence is a criticality sequence consisting of a uranium solution spill due to improper preventive maintenance on a pump, followed by the loss of moderation control due to inadvertent sprinkler activation before the spill can be cleaned up.

Use of Tables A-9, A-10, and A-11 of NUREG-1520

As illustrated above, an accident sequence consists in general of an initiating event with a certain frequency followed by a number of subsequent events. While the number and type of events making up the sequence may vary, the likelihood indices of the individual events are combined, with appropriate consideration for duration of failure and demand rate, to arrive at a likelihood index for the accident sequence as a whole. The basic steps in this process are outlined below:

1. Determine the events making up the sequence (initiating event and subsequent failures).

2. Determine whether the event is characterized by a frequency of occurrence (f-type) or a PFOD (p-type). If an f-type event, use Table A-9 to assign the indices. If a p-type event, use Table A-10 to assign the indices.

3. If the initiating event is a p-type event, take the demand rate into account to modify the indices from Table A-9.

4. If the subsequent event is an f-type event, take the duration index for the initiating event into account from Table A-11.

5. Combine the appropriate indices into an overall accident sequence likelihood index.

The table below provides a summary of how Tables A-9, A-10, and A-11 may be used to determine overall accident sequence likelihood:

Initiator Type	Subsequent Event Type	Initiator Index	Subsequent Event Index	Duration Index	Accident Sequence Index
f-type	p-type	f1: Table A-9	p2: Table A-10	NA	f1 × p2
f-type	f-type	f1: Table A-9	f2: Table A-9	d1: Table A-11	f1 × d1 × f2
p-type	p-type	p1: Table A-10*	p2: Table A-10	NA	p1 × p2
p-type	f-type	p1: Table A-10*	f2: Table A-9	d1: Table A-11	p1 × d1 × f2

*To convert PFOD indices to frequency indices, use the indices of Table A-10 modified to take demand rate into account as follows:

Demand Rate	Modify Table A-10 index
Hundreds of times per year (daily)	Increase base index by 2
Tens of times per year (monthly)	Increase base index by 1
Once per year	Use base index
Once every ten years	Decrease base index by 1

Care must be taken in the use of these tables not to confuse frequency with probability. For example, assuming the initiating event occurs is often done because doing so is simpler and more conservative. This is not, however, equivalent to assigning an initiating event frequency of 1, which is an event which occurs once per year. The confusion of failure frequency (with units of inverse time) with probability (dimensionless) can lead to significant errors in the overall accident sequence likelihood.

Example: An accident sequence in which solution sampling prior to transfer to an unfavorable geometry tank is the initiating event. A single administrative control might have a probability

index of -2 (with appropriate management measures or redundancy). Similarly, if the historical data indicated a PFOD of 10^{-2}, an index of -2 would be appropriate. However, if this operation is a batch process conducted ten times per year, this results in an initiating event frequency of 10/yr × 10^{-2} (PFOD) = 10^{-1}/yr (for an index of -1). If the operation is conducted one hundred times per year, this results in an initiating event frequency of 100/yr × 10^{-2} (PFOD) = 10^{0}/yr (for an index of 0). Use of Table A-10 without any consideration of the demand rate would result in an index of -2.

Note that use of the incorrect table can also lead to erroneous results. Comparing the indices in Tables A-9 and A-10 for the same type of control (although this is not the only factor that should be considered), it is immediately seen that use of Table A-9 results in a higher index than from use of Table A-10. For example, a simple administrative control (without enhancing factors such as redundancy or large margin) would have a probability index of -1 to -2 using Table A-10, but a frequency index of 0 using Table A-9. This is intuitively reasonable because Table A-9 is for events characterized by a frequency (which must be present on a continuous basis) and Table A-10 is for events which are only demanded under certain conditions (which must be present on occasion).

Additional Considerations in the Use of Index Tables

As stated in the discussion of initiating events in the text of the ISG, assignment of a qualitative score may be based either upon objective evidence of the frequency of occurrence or upon certain qualitative characteristics of the process or facility (availability and reliability qualities). In accordance with this, Tables A-9 and A-10 of NUREG-1520 contain two columns that represent two different methods for assigning likelihood indices. As stated in the introduction to Appendix A, this is a semi-quantitative method that allows for the use of quantitative information, if available.

For initiating events that are external events or internal events other than IROFS failures, the column entitled “Based on Evidence” in Table A-9 should be employed in assigning indices. For IROFS failures to which Table A-9 is applicable, either the column entitled “Based on Evidence” or “Based on Type of IROFS” may be employed. Because the type of IROFS is only one of the availability and reliability qualities upon which likelihood depends, the footnote to this table indicates that the index scores applicable to a particular type of IROFS can be one value higher or lower than the index shown.[1] Thus, other specific availability and reliability qualities (as discussed in NUREG-1520, Section 3.4.3.2(9)) should be considered in assigning the final likelihood index.[2] In the absence of sufficiently detailed information with regard to these factors, appropriate conservatism should be used in assigning indices (e.g., using the highest index in

[1]The title “Based on Type of IROFS” is somewhat of a misnomer, in that several of the criteria also include consideration of redundancy, margin, and independence. Indices based solely on the type of IROFS would cover an even broader range.

[2]This is consistent with the caveat for Table A-4, that such coarse criteria is only useful for screening purposes or making an initial estimate of the likelihood. Because IROFS meeting these criteria can have a broad range of reliability, management measures applied to all the availability and reliability qualities of the IROFS should be taken into account in assigning the likelihood indices.

the range). Because of the large uncertainty associated with basing likelihood on the type of IROFS, historical and/or operating evidence should be used to assign indices whenever available. The same considerations discussed above should be employed when using Table A-10 to assign likelihood indices.

The presence of two columns should not be construed to mean that the two sets of criteria may be considered equivalent except in a rough, order-of-magnitude sense (e.g., a single passive engineered IROFS does not necessarily have a PFOD of 10^{-3} to 10^{-4}). This is because the type of IROFS is only one of the availability and reliability qualities that must be considered.

Appropriate use of Tables A-9 and A-10 to assign likelihood indices also requires that attention be given to the footnotes and comments in these tables. As indicated in the footnotes, indices less than -1 should not be used unless the management measures are of high quality. This is because even though a passive engineered control may have high inherent reliability while it is installed, this could be easily defeated by a poor configuration management program, which is administrative in nature (as are all management measures). Justification should be provided as to why the management measures are of high quality. Also, justification should be given in the ISA Summary whenever a range of indices is possible and the more negative index is used. As alluded to in the comments, the more negative the index, the more justification is required. As indicated, indices of -4 and -5 can rarely be justified by evidence. Use of these indices requires substantial justification that the IROFS are exceptionally robust.

The assignment of failure duration indices using Table A-11 should also be based on objective criteria (such as documented mean time to repair (MTTR) or surveillance periods established in plant procedures).

In using demand rates to modify probability indices from Table A-10, conservative estimates of the demand rate should be used and the basis for this estimate documented, and if they could credibly be changed, controlled. For example, the time needed to fill a cylinder may depend on inherent physical laws and would not need specific controls. However, if the number of batches is limited by the maximum allowed inventory, this should be controlled by the license or by plant procedures.

Description of Accident Sequences and IROFS

Tables A-12 and A-13 include descriptions of accident sequences and IROFS. These must be sufficiently clear to permit the reviewer to understand the sequence of events needed for an accident to occur and how the controls established prevent the sequence from occurring. The initial failure and all subsequent failures necessary for the sequence to progress to the ultimate consequences (an accident exceeding the consequence thresholds in 10 CFR 70.61) should be specified. In addition, any initial conditions credited in meeting the performance requirements should be specified. If important to the likelihood of the sequence, the order in which these events occurs should be specified. For example, in Table A-12, sequence PPB2-1C is the reverse of the events in sequence PPB2-1A. When failure duration indices are taken into account, these pertain to the initiating event; therefore, the accident sequence likelihood is dependent on which event occurs first.

In describing IROFS, it is important that the safety function performed by the IROFS, and the attributes of the IROFS necessary to perform the safety function be specified. For example, for

the first IROFS in Table A-13, the safety function is preventing mass from accumulating outside the hopper. Therefore, the only attribute of IROFS PPB2-C1 that is required to be specified is that it be designed to prevent leaks, including use of a double gasket at its outlet. Because the material of composition, size, and other attributes of the hopper have no role in preventing this accident sequence, they are not required to be specified. The second IROFS is an example of a system of IROFS that collectively provides for moderation control (i.e., dual sampling, administrative exclusion of water, double piping, floor drains, and roof integrity). As with the first IROFS, the size of the piping is not significant; only the fact that there is double piping is important to preventing this accident sequence. A sufficient level of detail should be specified to provide assurance that safety-significant aspects of the IROFS are recognized and appropriately controlled. However, an excessive amount of detail could lead to obscuring the safety-significant aspects of IROFS and could lead to unnecessary and burdensome changes to the ISA and ISA summary. IROFS may be specified as the sub-component level, component level, or system level, as appropriate. For example, it it not necessary to specify every geometry limited pipe in the building as an IROFS. If the safety function is to maintain geometry control, it would be sufficient to specify a systems-level IROFS with the description "All fissile material piping in the solution recovery area will be less than 2-inches in diameter."

It may be that a single piece of equipment performs several different safety functions and is credited in several different accident sequences. In such cases, it must be clear in the accident sequence description what safety function and attribute of the IROFS is being credited, as well as what failure mode of the IROFS leads to the accident.

Summary Table of Accident Sequences

Table A-7 of NUREG-1520 contains a summary table of several accident sequences for a powder blending process. This is but one way to display the information on accident sequences obtained during performance of the ISA. As shown in Appendix A of NUREG-1718, "Standard Review Plan for the Review of an Application for a Mixed Oxide Fuel Fabrication Facility," a fault tree (quantitative or qualitative) may also be used, as may other formats. The important information that must be conveyed, however, is a list of accident sequences, identification of the initiating event, the set of subsequent events leading to the accident and the IROFS that prevent them, the likelihood of the initiating event and subsequent failures, the ultimate consequence category, and the overall assessment of compliance with the performance requirements (e.g., total risk index). Any other information that is needed to demonstrate that the performance requirements are met should also be specified (e.g., initial conditions, demand rate, duration indices, index modification for dependent failures). Note that there are two types of accident sequences in this table: (1) two sequences initiated by IROFS failures (both f-type initiating events with f-type subsequent failures, and crediting duration indices), and (2) two sequences initiated by internal events other than IROFS failures (and crediting initiating event frequency).

While this guidance follows the structure of Appendix A of NUREG-1520, it is also applicable to Appendix A of NUREG-1718.