APPENDIX A

Field Code Changed

EXAMPLE PROCEDURE FOR ACCIDENT SEQUENCE EVALUATION

This appendix provides the U.S. Nuclear Regulatory Commission (NRC) reviewer with an example of one method of evaluating accident sequences for compliance with the likelihood requirements of 10 CFR 70.61. It employs a semi-quantitative risk index method for categorizing accident sequences in terms of their likelihood of occurrence and their consequences of concern. The risk index method framework will enable the applicant to identify, and the NRC reviewer to confirm, which accident sequences have consequences that exceed the performance requirements of Title10, Section 70.61, "Performance Requirements," of the *Code of Federal Regulations* (10 CFR 70.61) and, therefore, require designation of items relied on for safety (IROFS) and supporting management measures. The ISA summary should include descriptions of these general types of higher consequence accident sequences.

This appendix presents an example of how the risk index method can be applied to a uranium powder blender. It describes one method of evaluating compliance with the consequence and likelihood performance requirements of 10 CFR 70.61. The method is intended to permit any available quantitative information to be considered. For consistency, the NRC reviewer's approach could also include assigning quantitative values to any qualitative likelihood assessments made by an applicant since likelihoods are inherently quantitative. This method should not be interpreted as a requirement that an applicant use quantitative evaluation. However, evaluation of a particular accident should be consistent with any facts available, which may include quantitative information concerning the availability and reliability of IROFS involved.

This appendix is not a "format and content guide" for either the ISA or the ISA summary. It simply presents one method of analysis and categorization of credible accident sequences for facility processes. The method described in this appendix uses both qualitative and quantitative criteria for evaluating frequency indices of safety controls. These criteria for assigning indices, particularly the descriptive criteria provided in some tables of this appendix, are intended to be examples, not universal criteria. It is preferable that each applicant develop such criteria based on particular types of IROFS and management measure programs. The applicant should modify and improve such criteria as insights are gained during performance of the ISA.

If the applicant evaluates accidents using a different method, the method should produce similar results in terms of how accidents are categorized. The method should be regarded as a screening method, not as a definitive method of proving the adequacy or inadequacy of the IROFS for any particular accident. Because methods can rarely be universally valid, individual accidents for which this method does not appear applicable may be justified by an evaluation using other methods. The method does have the benefit that it evaluates, in a consistent manner, the characteristics of IROFS used to limit accident sequences. This will permit identification of accident sequences with defects in the combination of IROFS used. Such IROFS can then be further evaluated or improved to establish adequacy. The procedure also ensures the consistent evaluation of similar IROFS by different ISA teams. Sequences or IROFS that have risk significance and are evaluated as marginally acceptable are good candidates for more detailed evaluation by the applicant and the reviewer.

The tabular accident summary resulting from the ISA should identify, for each sequence, the engineered or administrative IROFS that must fail to allow the occurrence of consequences that

exceed the levels identified in 10 CFR 70.61. Chapter 3 of this Standard Review Plan (SRP) specifies acceptance criteria for these IROFS and for meeting the performance requirements of 10 CFR 70.61. These criteria require that IROFS be sufficiently unlikely to fail. However, the acceptance criteria do not explicitly mandate any particular method for assessing likelihood. The purpose of this appendix is to provide an example of an acceptable method to perform this evaluation of likelihood.

A.1 Risk Matrix Development

Consequences

The regulation in 10 CFR 70.61 specifies two categories for accident sequence consequences: "high consequences" and "intermediate consequences." Implicitly there is a third category for accidents that produce consequences less than "intermediate." This category will be referred to as "low consequence" accident sequences. The primary purpose of process hazard analysis (PHA) is to identify all uncontrolled and unmitigated accident sequences. These accident sequences can then be categorized into one of these three consequence categories (high, intermediate, low) based on their predicted radiological, chemical, and/or environmental impacts. Although the subsequent ISA analysis focuses only on those accident sequences having high or intermediate consequences, by identifying and tabulating low consequence events in the ISA, the reviewer can evaluate the completeness of the PHA and ISA analyses. Table A-1 presents the radiological and chemical consequence severity limits of 10 CFR 70.61 for each of the three accident consequence categories.

Table A-1: Consequence Severity Categories Based on 10 CFR 70.61

	Workers	**Offsite Public**	**Environment**
Category 3 High Consequence	*RD> 1 Sievert (Sv) (100 rem) **CD = endanger life	RD> 0.25 Sv (25 rem) 30 milligrams (mg) sol U intake CD = long-lasting health effects	
Category 2 Intermediate Consequence	0.25 Sv (25 rem) <RD≤ 1 Sv (100 rem) CD = long-lasting health effects	0.05 Sv (5 rem) <RD≤ 0.25 Sv (25 rem) CD = mild transient health effects	Radioactive release >5000 x Table 2 of 10 CFR Part 20, Appendix B
Category 1 Low Consequence	Accidents of lower radiological and chemical exposures than those above in this column	Accidents of lower radiological and chemical exposures than those above in this column	Radioactive releases producing lower effects than those referenced above in this column

* RD = Radiological Dose
** CD = Chemical Dose

Likelihood

10 CFR 70.61 also specifies the permissible likelihood of occurrence of accident sequences of different consequences. "High consequence" accident sequences must be "highly unlikely" and "intermediate consequence" accident sequences must be "unlikely." Implicitly, accidents in the

"low consequence" category can have a likelihood of occurrence less than "unlikely" or simply "not unlikely." Table A-2 shows the likelihood of occurrence limits of 10 CFR 70.61 for each of the three likelihood categories.

Table A-2: Likelihood Categories Based on 10 CFR 70.61

	Qualitative Description
Likelihood Category 1	Consequence Category 3 accidents must be "highly unlikely"
Likelihood Category 2	Consequence Category 2 accidents must be "unlikely"
Likelihood Category 3	Consequence Category 1 accidents may be "not unlikely"

Risk Matrix

The three categories of consequence and likelihood can be displayed as a 3 x 3 risk index matrix. By assigning a number to each category of consequence and likelihood, a qualitative risk index can be calculated for each combination of consequence and likelihood. The risk index equals the product of the integers assigned to the respective consequence and likelihood categories. Table A-3 illustrates the risk index matrix, along with computed risk index values. The shaded blocks identify accidents for which the consequences and likelihoods yield an unacceptable risk index and to which IROFS must be applied.

Table A-3: Risk Matrix with Risk Index Values

Severity of Consequences	Likelihood of Occurrence		
	Likelihood Category 1 Highly Unlikely (1)	Likelihood Category 2 Unlikely (2)	Likelihood Category 3 Not Unlikely (3)
Consequence Category 3 High (3)	Acceptable Risk 3	Unacceptable Risk 6	Unacceptable Risk 9
Consequence Category 2 Intermediate (2)	Acceptable Risk 2	Acceptable Risk 4	Unacceptable Risk 6
Consequence Category 1 Low (1)	Acceptable Risk 1	Acceptable Risk 2	Acceptable Risk 3

The risk indices can initially be used to examine whether the consequences of an uncontrolled and unmitigated accident sequence (i.e., without any IROFS) could exceed the performance requirements of 10 CFR 70.61. If the performance requirements could be exceeded, the applicant must designate IROFS to prevent the accident or to mitigate its consequences to an acceptable level. A risk index value less than or equal to four (4) means the accident sequence

is acceptably protected against and/or mitigated. If the applicant provides this risk index in the ISA and ISA Summary, the reviewer can quickly scan these data to confirm that each accident sequence meets the performance requirements of 10 CFR 70.61.

If the risk index of an uncontrolled and unmitigated accident sequence exceeds 4, the likelihood of the accident must be reduced through designation of IROFS. In this risk index method the likelihood index for the uncontrolled and unmitigated accident sequence is adjusted by subtracting a score corresponding to the type and number of IROFS that have been designated. Table A-4 lists the qualitative scores assigned to the four types of IROFS.

Reviewers should note that the qualitative scores assigned in Table A-4 are for illustrative purposes only. IROFS meeting the criteria for a particular score in Table A-4 could have a wide range of availability or reliability. Such coarse criteria are useful for screening purposes, but when the total evaluated likelihood score for an accident sequence lies near the acceptance guideline value, a more careful evaluation should be done. Such evaluations should consider the management measures applied to all the reliability and availability qualities of the IROFS, or system of IROFS, protecting against the accident, as explained in the likelihood acceptance criteria of Section 3.4.3.2.

Table A-4: Qualitative Categorization of IROFS

Numeric Value	Description of IROFS
1	Protection by a single trained operator with adequate response time **(Administrative IROFS)**
2	Protection by a single active engineered IROFS, functionally tested on a regular basis **(Active Engineered IROFS)**
3	Protection by a single passive-engineered IROFS, functionally tested on a regular basis, or by an active engineered IROFS with a trained operator for back-up **(Passive Engineered IROFS or Combined Engineered and Administrative IROFS)**
4	Protection by two independent and redundant engineered IROFS, as appropriate, functionally tested on a regular basis **(Combination of Two Active or Passive Engineered IROFS)**

To demonstrate compliance with the performance requirements of 10 CFR 70.61, the ISA should assign a consequence category to each identified accident sequence. The likelihood of occurrence of those accident sequences identified as high or intermediate consequence events must then be assigned to one of the three likelihood categories. To be acceptable, the controlled and/or mitigated accident consequences and likelihoods must have valid bases, and the applicant must include the bases for all general types of high and intermediate consequence accident sequences in the ISA Summary.

A.2 Consequence Category Assignment

Categorization of an accident sequence as a high-consequence event or an intermediate-consequence event, or neither, is based on the estimated consequences of prototype accidents. Although accident consequences can be determined by actual calculations, calculations need not be performed for each individual accident sequence listed for a process. Accident consequences may also be estimated by comparison to similar events for which reasonably bounding conservative calculations have been made. Categorization also requires consideration of acute chemical exposures that an individual could receive from licensed material or hazardous chemicals incident to the processing of licensed material. The applicant must select appropriate acute chemical exposure data and relate these data to the performance requirements of 10 CFR 70.61(b)(4) and (c)(4). In this appendix, the Acute Exposure Guideline Level (AEGL) and Emergency Response Planning Guideline (ERPG) are used. AEGL-3 and ERPG-3 levels are life-threatening.

Consequence Category 3 (High-Consequences) includes accidents resulting in any consequence specified in 10 CFR 70.61(b). These include (1) acute worker exposures of (a) radiation doses greater than 1 Sievert (100 rem) total effective dose equivalent (TEDE), and (b) chemical exposures that could endanger life (above AEGL-3 or ERPG-3), and (2) acute exposures to members of the public outside the controlled area to (a) radiation doses greater than 0.25 Sievert (25 rem) TEDE, (b) soluble uranium intakes greater than 30 milligram, and (c) chemical exposures that could lead to irreversible or other serious long-lasting health effects (exceeding AEGL-2 or ERPG-2). An unshielded nuclear criticality would normally be considered a “high consequence” event because of the potential for producing a high radiation dose to a worker.

Consequence Category 2 (Intermediate-Consequences) includes accidents resulting in any consequence specified in 10 CFR 70.61(c). These include (1) acute exposures of workers to (a) radiation doses between 0.25 Sievert (25 rem) and 1 Sievert (100 rem) TEDE, and (b) chemical exposures that could lead to irreversible or other serious long-lasting health effects above AEGL-2 or ERPG-2), and (2) acute exposures of members of the public outside the controlled area to (a) radiation doses between 0.05 Sievert (5 rem) and 0.25 Sievert (25 rem) TEDE, (b) chemical exposures that could cause mild transient health effects (exceeding AEGL or ERPG-1), and (3) release of radioactive material outside the restricted area that would, if averaged over a 24-hour period, exceed 5000 times the values specified in Table 2 of Appendix B to 10 CFR Part 20.

Consequence Category 1 (Low-Consequences) includes accidents with potential adverse radiological or chemical consequences, but at exposures less than Categories 3 and 2.

This system of consequence categories is shown in Table A-5.

Table A-5: Consequence Severity Categories Based on 10 CFR 70.61

	Workers	Offsite Public	Environment
Category 3 High Consequence	*RD>1 Sievert (Sv) (100 rem) **CD>AEGL-3, ERPG-3	RD>0.25 Sv (25 rem) 30 mg sol U intake CD>AEGL-2, ERPG-2	
Category 2 Intermediate Consequence	0.25 Sv (25 rem) <RD≤ 1 Sv (100 rem) AEGL-2, ERGP-2 <CD≤ AEGL-3, ERPG-3	0.05 Sv(5 rem) < RD≤ 0.25 Sv (25 rem) AEGL-1, ERGP-1 <CD≤ AEGL-2, ERPG-2	Radioactive release > 5000 x Table 2 Appendix B of 10 CFR Part 20
Category 1 Low Consequence	Accidents of lower radiological and chemical exposures than those above in this column	Accidents of lower radiological and chemical exposures than those above in this column	Radioactive releases with lower effects than those referenced above in this column

* RD - Radiological Dose
**CD - Chemical Dose

The applicant should document the bases for bounding calculations of the consequence assignment in the ISA Summary submittal. NUREG/CR-6410, "Nuclear Fuel Cycle Facility Accident Analysis Handbook," March 1998, describes valid methods and data that may be used by the applicant or staff for confirmatory evaluations.

A.3 Likelihood Category Assignment

An assignment of an accident sequence to a likelihood category is acceptable if it is based on the record of occurrences at the facility, the record of failures of IROFS at the facility, on applicable event data for similar systems, on objective qualitative criteria governing system failure rates and availability, or on other methods that have objective validity. Because sequences leading to accidents often involve multiple failures, the likelihood of the whole sequence will depend on the frequencies of initiating events and failure likelihoods of engineered and administrative IROFS. The method of likelihood assignment used in this appendix relies on the expert engineering judgment of the analyst and includes assessment of the number, type, independence, and observed failure history of designated IROFS. Engineered and administrative IROFS, even those of the same types, have a wide range of reliability. By requiring explicit consideration of most of the underlying events and factors that significantly affect the likelihood of the accident and explicit criteria for assigning likelihood, greater consistency in assigning likelihood to accident sequences across different systems within a facility and among different applicants should be possible.

This section provides one example of a set of acceptable semi-quantitative risk guidelines for determining compliance with the likelihood requirements of 10 CFR 70.61 when using methods of evaluation that are either quantitative or use the risk index method outlined in this appendix.

The performance criteria of 10 CFR 70.61 are formulated in terms of likelihood limits on each event sequence separately. The example guidelines given in Table A-6 were based on the acceptance criteria guidance on likelihood definitions given in Section 3.4.3.2 of this chapter.

Table A-6: Example Likelihood Index Limit Guidelines

	Likelihood Category	Event Frequency limits*	Risk Index limits
Not Unlikely	3	more than10^{-4} per-event/yr	> -4
Unlikely	2	between 10^{-4} and 10^{-5} per-event/yr	-4 to -5
Highly Unlikely	1	less than 10^{-5} per-event per-year	≤ -5

Any risk or risk index method of likelihood evaluation using criteria as simple as those provided in the example method in this appendix should not be relied on exclusively to make decisions as to the acceptability of the likelihood of a given event sequence. Consideration of qualitative criteria, such as degree of defense-in-depth or independence of controls, may be used to alter decisions based on the example simple semi-quantitative criteria presented here.

A.4 Assessing Effectiveness of IROFS

The risk of an accident sequence is reduced through application of different numbers and types of IROFS. By either reducing the likelihood of occurrence or by mitigating the consequences, IROFS can reduce the overall resulting risk. The designation of IROFS should generally be made to reduce the likelihood (i.e., prevent an accident), but the consequences may also be reduced by minimizing the potential hazards (e.g., quantity) if practical. Based on hazards identification and accident sequence analyses for which the resulting unmitigated or uncontrolled risks are unacceptable, key safety controls (administrative and/or engineered IROFS) may be designated as IROFS to reduce the likelihood of occurrence and/or mitigate the consequence severity.

The accident evaluation method described below does not preclude the need to comply with the double-contingency principle for sequences leading to criticality (see 10 CFR 70(a)(9) and Chapter 5 of this SRP).

A.5 Example Risk Index Evaluation Method

As previously mentioned, one acceptable way for the applicant to present the results of the ISA is a tabular summary of the identified accident sequences. Table A-7 is an acceptable format for such a table. This table lists several example accident sequences for a powder blender at a typical facility. Table A-7 summarizes two sets of information: (1) the accident sequences identified in the ISA; and (2) a risk index, calculated for each sequence, to show compliance with the regulation. This risk index is a representation of the frequency of the accident

sequence in accordance with the mathematics underlying accidents resulting from sequences of events. This underlying mathematics is described in the following section.

Field Code Changed

A.5.1 Mathematics of Accident Sequence Frequencies and the Risk Index Method

10 CFR 70.61 requires that controls be applied so that 'high consequence' events are 'highly unlikely', and 'intermediate consequence' events 'unlikely'. This means that each accident sequence, consisting of initiating events and subsequent events, that leads to "high consequences" must be "highly unlikely". In quantitative terms "highly unlikely" will be treated here in terms of annual frequency of occurrence. The purpose of this section is to explain the concepts and mathematical formulae underlying the risk index method of likelihood evaluation, which is given in Appendix A as one example of an acceptable method for such evaluations in ISAs.

Since high consequence events are, for workers, potentially life threatening or fatal, "highly unlikely" must be taken to mean quite low frequency. Generally achieving such low frequency requires either redundancy, robust passive control with large safety margin, or rare external events. Redundancy of safety controls is a method for limiting the occurrence rate of accidents by applying controls such that two coincident failure conditions must exist for a high consequence event to occur. Use of redundant controls is common in criticality safety, where the double contingency principle is a standard. There are different types of redundant control systems. The effectiveness of each of these systems depends not just on having controls with low failure rates, but also on limiting down time after failure occurs. Down time, or the period of vulnerability resulting from an event, may be limited due to inherent fail-safe or failure-evident nature of the event. For events which lack these properties, failure must be detected, either by hardware monitoring or by surveillance testing, which is usually part of the plant preventive maintenance program. To understand how accident frequencies depend on frequency of failure events and down time, let us define the following symbols:

λ_i = rate of failure of control i or of occurrence of initiating event i (in units of per year)
t = mean time to failure (MTTF) = $1/\lambda_i$ = mean up time
T_i = mean down time of control i = $1/\mu_i$
u_i = unavailability of control i
sfr = system failure rate (accident rate)

Mean down time is often not the same as mean time to actually repair the affected safety system (MTTR), but rather the mean that the system is vulnerable to the second failure. This may be considerably shorter than the MTTR, if there is an alternative means of placing the system in a state as safe as with the unfailed control.

Unavailability, u, is defined as the probability that a control or system is not available to perform its function at a particular time. Unavailability is usually the predominant component of probability of failure of a system on demand. The normal model is that a control or system is either in an unavailable ("down") state, or an available ("up") state. The system randomly changes from one state to the other over time, governed by the failure rate λ and the repair rate $\mu = 1/T$. As a long run average the unavailability of a control is thus the fraction of the time that it is "down"; which is the ratio of down time to down time plus up time:

$u = T/(t+T)$

For any reasonably available system, up-time is much greater than downtime, $t >> T$.

Thus approximately: $u \approx T/t$

and $t = 1 / \lambda$, so: $u \approx \lambda T$

There are different types of redundant control systems. Three of the most common have the following equations for their system failure rate (accident rate):

two continuous parallel controls: $sfr = \lambda_1 u_2(1 - u_1) + \lambda_2 u_1(1 - u_2)$
usually approximated as: $sfr \approx \lambda_1 u_2 + \lambda_2 u_1 \approx \lambda_1(\lambda_2 T_2) + \lambda_2(\lambda_1 T_1)$
Equation (1)

three continuous parallel controls: $sfr = \lambda_1 u_2 u_3(1 - u_1) + \lambda_2 u_1 u_3(1 - u_2) + \lambda_3 u_1 u_2(1 - u_3)$
usually approximated as: $sfr \approx \lambda_1 u_2 u_3 + \lambda_2 u_1 u_3 + \lambda_3 u_1 u_2$ Equation (2)

challenging initiating event of frequency λ_1 with one control: $sfr = \lambda_1 u_2$ Equation (3)

initiating event i with 2 redundant standby identical controls: $sfr = \lambda_i u_1 u_2$ Equation (4)

The system of frequency and probability (of failure on demand) described in this appendix is based on taking the logarithm of each of the terms in the above equations. Thus for Equation (1) in log space two terms would correspond to the two accident sequences by which the system could fail, namely control 1 first or control 2 first:

sequence 1: $\log(\lambda_2) + \log(u_1)$
sequence 2: $\log(\lambda_1) + \log(u_2)$

Or if only failure rates λ and down times T are used, then, with the approximation $u \approx \lambda T$, the formulae corresponding to Equation (1) above become:

$sfr = \lambda_1(\lambda_2 T_2) + \lambda_2(\lambda_1 T_1)$

sequence 1: $\log(\lambda_2) + \log(\lambda_1) + \log(T_1)$
sequence 2: $\log(\lambda_1) + \log(\lambda_2) + \log(T_2)$

Thus, for two continuous redundant controls, two accident sequences are typically scored for likelihood. One of the two will usually have a larger frequency, so it is important to evaluate both. For situations modeled by Equation (3) above, there would be just one term.

Table A-9 below provides one example of criteria that might be used to assign frequency index numbers (log(frequency) = log(λ)). Table A-10 provides one example of criteria that might be used to assign index numbers for probabilities of failure on demand (log(unavailability) = log(u)). Table A-11 provides one example of criteria for assigning index numbers for down time, that is, logarithm of durations of vulnerability, log(T). Note that when MTTF >> MTTR, $u = \lambda T$ approximately, so that the values λ from Table A-9 and the values T from Table A-11 can be combined to obtain u for a given control if λ and T are the known quantities.

The “average” down time, when determined by surveillance, is dependent on the interval of time between scheduled system surveillance tests. If a surveillance test is done weekly, then, when the system is found to be in a failed state, the time that it could have been in this state is between zero and one week. Thus the average time that the system will have been down, when discovered by the test, is half this, or 3.5 days. In units of per year this is 3.5/365 = 0.01 year, and log(.01) = -2. Thus short surveillance interval can considerably reduce the system failure rate.

A.5.2 An Example Application of a Risk Index Method of Likelihood Evaluation

Accident sequences result from initiating events, followed by failure of one or more IROFS. Thus, Table A-7 has columns for the initiating event and for IROFS. The initiating event may be failure of one of the IROFS. IROFS may be mitigative or preventive. Mitigative IROFS are measures that reduce the consequences of an accident. In accordance with Tables A-9 through A-11, index numbers are assigned to initiating events, IROFS failure events, and mitigation failure events, based on the reliability characteristics of these items.
As an example, with two redundant IROFS there is an accident sequence in which an initiating failure of one IROFS places the system in a vulnerable state. While the system is in this vulnerable state, the second IROFS may fail, which would result in an accident with consequences exceeding the criteria in 10 CFR 70.61. For such sequences the frequency of the accident depends on three quantities: the frequency of the first event, the duration of vulnerability, and the frequency of the second IROFS failure. For this reason, the duration of the vulnerable state should be considered, and a duration index should be assigned. The values of all index numbers for a sequence are added to obtain a total likelihood index, T. In this risk index method of evaluation, accident sequences are then assigned to one of the three likelihood categories of the risk matrix, depending on the value of this index in accordance with Table A-8.

The values of index numbers in accident sequences are assigned considering the criteria in Tables A-9 through A-11. Each table applies to a different type of event. Table A-9 applies to events that have *frequencies* of occurrence, such as initiating events, which may be IROFS failures or external events. When failure *probabilities* are required for an event subsequent to the initiating event, Table A-10 provides the index values. Table A-11 provides index numbers *for durations* of failure. These are used in cases where information on probability of failure on demand is not available for the IROFS failures subsequent to the initiating event. Note the third row in Table A-7; it evaluates the reverse sequence to that in row 1. That is, the second IROFS fails first. This should be considered as a separate accident sequence, because, as shown, it may have a different frequency.

Table A-7: Example Accident Sequence Summary and Risk Index Assignment
Process: uranium dioxide(UO_2) powder preparation (PP); Unit Process: additive blending;
Node: blender hopper node (PPB2)

Accident Identifier A	Initiating Event or IROFS 1 failure B	Preventive Safety Parameter 2 or IROFS 2 Failure/Success C	Mitigation IROFS Failure/ Success D	Likelihood* Index T E=B+C+D	Likelihood Category F	Consequence Category G	Risk Index H=F+G	Comments & Recommendations
PPB2-1A (Criticality from blender leak of UO_2)	PPB2-C1: Mass Control Failure: Blender leaks UO_2 onto floor, critical mass exceeded Frq1 = -1 Dur1 = -4	PPB2-C2: Moderation Failure: Suffic. Water for criticality introduced while UO_2 on floor: Frq2 = -2	N/A	T = -7	1	3	4	Criticality, consequences = 3 IROFS 2 fails while IROFS 1 is in failed state. T = -1-4-2 = -7
PPB2-1B (Rad. release from blender leak of UO_2)	PPB2-C1: Mass Control fails but critical mass not exceeded Frq1=-1 Dur1 N/A	PPB2-C2: N/A	Ventilation Failure: Ventilated blender enclosure Prf = -3	T = -4	1	2	3	Rad consequences, no criticality unmitigated sequence: IROFS 1 & mitigation fail. T= -1-3 = -4
PPB2-1C (criticality from blender presence of water under blender)	PPB2-C2: Moderation Failure: Suffic. water for criticality on floor under UO_2 blender Frq1 = -2 Dur1 = -3	PPB2-C1: Mass Control Failure: Blender leaks UO_2 on floor while water present Frq2 = -1	N/A	T = -6	1	3	4	Criticality by reverse sequence of PPB2-1A. Moderation fails first. Note different likelihood. T = -6

Table A-8: Likelihood Category Assignment

Likelihood Category	Likelihood Index T* (= sum of index numbers)
1	**T ≤ -5**
2	**-5 < T ≤ -4**
3	**-4 < T**

Table A-9: Failure Frequency Index Numbers

Frequency Index No.	Based on Evidence	Based on Type of IROFS**	Comments
-6 *	External event with freq. < 10^{-6} /yr		If initiating event, no IROFS needed.
-4 *	No failures in 30 years for hundreds of similar IROFS in industry	Exceptionally robust passive engineered IROFS (PEC), or an inherently safe process, or two independent active engineered IROFS (AECs), PECs, or enhanced admin. IROFS	Rarely justified by evidence. Further, most types of single IROFS have been observed to fail.
-3 *	No failures in 30 years for tens of similar IROFS in industry	A single IROFS with redundant parts, each a PEC or AEC	
-2 *	No failure of this type in this facility in 30 years	A single PEC	
-1	A few failures may occur during facility lifetime	A single AEC, an enhanced admin. IROFS, an admin. IROFS with large margin, or a redundant admin. IROFS	
0	Failures occur every 1 to 3 years	A single administrative IROFS	
1	Several occurrences per year	Frequent event, inadequate IROFS	Not for IROFS, just initiating events
2	Occurs every week or more often	Very frequent event, inadequate IROFS	Not for IROFS, just initiating events

* 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.
** Failure frequencies based on experience for a particular type of IROFS, as described in this column, may differ from values in column 1. In which case data from experience takes precedence.

Table A-10: Failure Probability Index Numbers

Probability Index No.	Probability of Failure on Demand	Based on Type of IROFS	Comments
-6*	10^{-6}		If initiating event, no IROFS needed.
-4 or -5*	10^{-4} - 10^{-5}	Exceptionally robust passive engineered IROFS (PEC), or an inherently safe process, or two redundant IROFS more robust than simple admin. IROFS (AEC, PEC, or enhanced admin.)	Rarely be justified by evidence. Most types of single IROFS have been observed to fail.
-3 or -4*	10^{-3} - 10^{-4}	A single passive engineered IROFS (PEC) or an active engineered IROFS (AEC) with high availability	
-2 or -3*	10^{-2} - 10^{-3}	A single active engineered IROFS, or an enhanced admin. IROFS, or an admin. IROFS for routine planned operations	
-1 or -2	10^{-1} - 10^{-2}	An admin. IROFS that must be performed in response to a rare unplanned demand	

*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.

Table A-11: Failure Duration Index Numbers

Duration Index No.	Avg. Failure Duration	Duration in Years	Comments
1	More than 3 years	10	
0	1 year	1	
-1	1 month	0.1	Formal monitoring to justify indices less than -1
-2	A few days	0.01	
-3	8 hours	0.001	
-4	1 hour	10^{-4}	
-5	5 minutes	10^{-5}	

As shown in Table A-11, the duration of failure, and thus the period the system is in a state of heightened vulnerability, is accounted for in establishing the overall frequency of the accident sequence. The period of vulnerability will normally be terminated by discovery of the vulnerable condition or failure; the system will then be rendered safe, either by removing the hazardous material, or by repairing or substituting for the safety function of the failed IROFS. The duration of this period of vulnerability is what determines the index value to be assigned from Table A-11.

For all these index numbers, the more negative the number, the lower the frequency of the event. Accident sequences may consist of varying numbers of events, starting with an initiating event. The total likelihood index is the sum of the indices for all the events in the sequence, including those for duration, except the initiating event, for which only the occurrence frequency index should be used. For example, a three event sequence would correspond to an event sequence frequency of the form $\lambda_1(\lambda_2 T_2)\ (\lambda_3 T_3)$, or five index values, three being frequencies, and two durations.

Consequences are assigned to one of the three consequence categories of the risk matrix, based on calculations or estimates of the actual consequences of the accident sequence. The consequence categories are based on the levels identified in 10 CFR 70.61. Multiple types of consequences can result from the same event. If there are multiple types of consequence, the consequence category is that for the most severe. Similarly, if a range of consequences could occur, then the highest consequence event of this range could occur, and if it falls in the "high consequence" range should be evaluated as such.

Table A-12 provides a more detailed description of the accident sequences used in the example of Table A-7. Such descriptive information may be necessary for the reviewer to understand the nature of the accident sequences listed in Table A-7.

Table A-13 is an example of one format for the descriptive list of IROFS required by the regulation. It should also include external initiating events that appear in the accident sequences and whose frequencies are relied on in demonstrating that the overall accident sequence frequency complies with the likelihood requirements. The information in Table A-13 on IROFS should have sufficient information and detail to permit the reviewer to understand why the initiating events and IROFS listed in Table A-7 have the frequency, unavailability, or duration indices assigned. Thus, Table A-13 may also contain such information as (1) the margins to safety limits, (2) the redundancy of an IROFS, and (3) the measures taken to ensure adequate reliability of an IROFS, if this information is necessary to understand the reliability and safety function of the IROFS with respect to the likelihood performance requirements.

Table A-12: Accident Sequence Descriptions

Process: uranium dioxide (UO_2) powder preparation (PP)
Unit: additive blending
Node: blender hopper node (PPB2)

Accident (see Table A-6)	Description
PPB2-1A Blender UO_2 leak criticality	The initial failure is a blender leak of UO_2 that results in a mass sufficient for criticality on the floor. (This event is not a small leak.) Before the UO_2 can be removed, moderator sufficient to cause criticality is introduced. Duration of critical mass UO_2 on floor estimated to be 1 hour.
PPB2-1B Blender UO_2 leak, rad. release	The initial failure is a blender leak of UO_2 that results in a mass insufficient for criticality on the floor or a mass sufficient for criticality but moderation failure does not occur. Consequences are radiological, not a criticality. A ventilated enclosure should mitigate the radiological release of UO_2. If It fails during cleanup or is not working, unmitigated consequences occur.
PPB2-1C	The events of PPB2-1A occur in reverse sequence. The initial failure is introduction of water onto the floor under the blender. Duration of this flooded condition is 8 hours. During this time, the blender leaks a critical mass of UO_2 onto the floor. Criticality occurs.

Table A-13: Descriptive List of IROFS

Process: uranium dioxide (UO_2) powder preparation (PP) Unit: additive blending
Node: blender hopper node (PPB2)

IROFS Identifier	Safety Parameter and Limits	IROFS Description	Max Value of Other Parameters	Reliability Management Measures	Quality Assurance Grade
PPB2-C1	Mass outside hopper: zero	Mass outside hopper: Hopper and outlet design prevent UO_2 leaks, double gasket at outlet	Full water reflection, enrichment 5%	Surveillance for leaked UO_2 each shift	A
PPB2-C2	Moderation: in UO_2 < 1.5 wt. % External water in area: zero	Moderation in UO_2: Two sample measurements by two persons before transfer to hopper External water: Posting excluding water, double piping in room, floor drains, roof integrity	Full water reflection, enrichment 5%	Drain, roof, and piping under safety-grade maintenance	A

Note: In addition to IROFS,, which are facility hardware and procedures, this table should include descriptions of external initiating events of which the low likelihood is relied on to achieve acceptable risk, especially those which are assigned frequency indices lower than -4. The descriptions of these initiating events should contain information supporting the frequency index value selected by
the applicant.

A.6 Determination of Likelihood Category in Table A-8

The likelihood category is determined by calculating the likelihood index, T, which equals the sum of the indices for the events in the accident sequence. Based on the calculated value of T, the likelihood category of each accident sequence can be determined from Table A-8.

A.7 Failure Probability Index Numbers in Table A-10

Occasionally, information concerning the reliability of an IROFS may be available as a probability on demand. That is, there may be a history of tests or incidents where the system in question is demanded to function. To quantify such accident sequences, the demand frequency, the initiating event, and the demand failure probability of the IROFS must be known. This table provides an assignment of index numbers for such IROFS in a way that is consistent with Table A-9. The probability of failure on demand may be the likelihood that it is in a failed state when demanded (availability) or that it fails to remain functional for a sufficient time to complete its function.

A.8 Management Measures for IROFS

Table A-13 is an acceptable way of listing IROFS in all the general types of accident sequences having consequences exceeding those identified in 10 CFR 70.61. The items listed should include all IROFS and all external events whose low likelihood of occurrence is relied on to meet the performance requirements of 10 CFR 70.61. For certain IROFS or accident sequences, to specify in the list of accident sequences or IROFS, information on management measures that is specific to that sequence or IROFS, in order to permit the reviewer to understand how the IROFS perform The reviewer examines this list to determine whether adequate management measures have been applied to each IROFS to ensure its continual availability and reliability, in conformance to 10 CFR 70.62(d). Management measures include such activities as maintenance, training, configuration management, audits and assessments, quality assurance, etc. Criteria for management measures are indicated in the baseline design criteria; others are described in greater detail in SRP Chapters 4 through 7 and Chapter 11. IROFS may have management measures applied in varying ways or to varying degrees, depending on the nature of the IROFS, and the degree of reliability assumed in demonstrating compliance with the likelihood requirements. This is the meaning of “graded management measures.”

A.9 Risk-Informed Review of IROFS

Column (h) in Table A-7 gives the risk indices for each accident sequence that was identified in the ISA. There are two indices, uncontrolled and controlled. The controlled index is a measure of risk without credit for the IROFS. If the uncontrolled risk index is a 6 or 9, while the controlled index is an acceptable value (4 or less), the set of IROFS involved are significant in achieving acceptable risk. That is, these IROFS have high risk significance. The uncontrolled risk index will be used by the reviewer(s) to identify all risk-significant systems of IROFS. These systems of IROFS will be reviewed more closely than IROFS established to prevent or mitigate accident sequences of low risk.

ANNEX TO APPENDIX A

Field Code Changed

USE OF APPENDIX A RISK INDEX METHODOLOGY

Introduction

The purpose of this annex is to clarify the proper use of theiik semi-quantitative index method as described in Appendix A to this report. Several licensees and applicants have used the index method of Appendix A (or a variation thereof) in performing their integrated safety analyses (ISAs). The U.S. Nuclear Regulatory Commission (NRC) reviews of these licensees' and applicants' ISA summaries have discovered 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, the index method is but one method of likelihood evaluation. The index method is not strictly a *qualitative* method, but is a *semiquantitative* 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 illustrates the logic 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. Otherwise, additional justification should be provided.

Likelihood Definitions

The likelihood definitions in Table A-6 of Appendix A are, as stated above, given 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, these values 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. Tables A-9, A-10, and A-11 of Appendix A present criteria for the assignment of the likelihood indices.

Appendix A 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. The interim staff guidance (ISG) provides examples of external and internal events that are not IROFS failures. IROFS failures characterized by a frequency of occurrence are those that are required to be continuously present, rather than those that 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 that are not required to be continuously present but that must perform a safety function on demand (subsequent to some process deviation or failure). Examples 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 sometimes be part of the initiating event.

In general, accident sequences may comprise many individual events. In general, accident sequences consist of an initiating event followed by the failure of one or more IROFS. Because the overall accident sequence likelihood must be consistent with the likelihood categories, it must have the same dimensional units as those of 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, the following considers only two-event sequences (in which the events are independent). The two basic kinds of events result in four basic types of two-event accident sequences, as described in the following sections.

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

In the index method of Appendix A, 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, 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 concurrently 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 considered.

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 resulting from the 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, 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. For the accident sequence likelihood to have the correct units (yr^{-1}), the demand rate of the first event must be considered.

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 before 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, 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 concurrently 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 considered.

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 that results from improper preventive maintenance on a pump, followed by the loss of moderation control because of inadvertent sprinkler activation before the spill can be cleaned up.

Use of Tables A-9, A-10, and A-11 in Appendix A

As illustrated above, an accident sequence generally consists 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 summarizes the use of Tables A-9, A-10, and A-11 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 10 years	Decrease base index by 1

Users of these tables must be careful not to confuse frequency with probability. For example, it is often assumed that the initiating event occurs 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 that 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: In this accident sequence, the initiating event is solution sampling before transfer to a tank with an unfavorable geometry. 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 10 times per year, this results in an initiating event frequency of $10/\text{yr} \times 10^{-2}$ (PFOD) = 10^{-1}/yr (for an index of -1). If the operation is conducted 100 times per year, this results in an initiating event frequency of $100/\text{yr} \times 10^{-2}$ (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.

Use of the incorrect table can also lead to erroneous results. A comparison of 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) immediately shows that use of Table A-9 results in a higher index than does 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 based on Table A-10, but a frequency index of 0 based on 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 that are demanded only 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 on objective evidence of the frequency of occurrence or on certain qualitative characteristics of the process or facility (availability and reliability qualities). In accordance with this, Tables A-9 and A-10 contain two columns that represent two different methods for assigning likelihood indices. As stated in the introduction to Appendix A, this is a semiquantitative 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 used in assigning indices. For IROFS failures to which Table A-9 applies, either the column entitled "Based on Evidence" or "Based on Type of IROFS" may be used. Because the type of IROFS is only one of the availability and reliability qualities on 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 Section 3.4.3.2(9) of this NUREG) should be considered in assigning the final likelihood index.[2] In the absence of sufficiently detailed information about these factors, appropriate conservatism should be used in assigning indices (e.g., using the highest index in 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.

---

[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, which warns that such coarse criteria are useful only 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 considered in assigning the likelihood indices.

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 control 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 deemed to be of high quality. Also, the ISA summary should justify the use of a more negative index whenever a range of indices is possible. As the comments suggest, 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 evidence 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 or surveillance periods established in plant procedures).

When the analysis uses 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 the rates 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 maximum allowed inventory limits the number of batches, this inventory 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 established controls 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 Title 10, Section 70.61, "Performance Requirements," of the *Code of Federal Regulations* (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 occur 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 considered, 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 to prevent mass from accumulating outside the hopper. Therefore, the only attribute of IROFS PPB2-C1 that must be specified is that it be designed to prevent leaks; such a design would include the use of a double gasket at the hopper's outlet. Because the material of composition, size, and other attributes of the hopper have no role in preventing this accident sequence, they need not 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 in the preceding example, the size of the piping is not significant; double piping is the only feature important to preventing this accident sequence. The level of detail should be

sufficient to provide assurance that safety-significant aspects of the IROFS are recognized and appropriately controlled. However, excessive 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 at the subcomponent level, component level, or system level, as appropriate. For example, it is 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."

A single piece of equipment may perform several different safety functions and be credited in several different accident sequences. In such cases, the accident sequence must clearly describe the safety function and attribute of the IROFS being credited, as well the failure mode of the IROFS that leads to the accident.

Summary Table of Accident Sequences

Table A-7 of Appendix A contains a summary table showing several accident sequences for a powder-blending process. This is one way to display the information on accident sequences obtained during performance of the ISA. As shown in Appendix A to NUREG-1718, "Standard Review Plan for the Review of an Application for a Mixed Oxide Fuel Fabrication Facility," issued August 2000, a fault tree (quantitative or qualitative) is one of the other formats that may be used. 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 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). Table A-7 shows two types of accident sequences: (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 to this report, it is also applicable to Appendix A to NUREG-1718.

APPENDIX B

Field Code Changed

QUALITATIVE CRITERIA FOR EVALUATION OF LIKELIHOOD

Purpose

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

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 Part 70 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 Chapter 3 of this NUREG, 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, "Natural Phenomena Hazards," provides additional guidance on the use of initiating events that are natural phenomena. Appendix C to Chapter 2, "Initiating Event Frequency," 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 Chapter 3 of this NUREG 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 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 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 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 definitions of "not credible" in Section 3.4.3.2(9) of this NUREG:

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

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 events 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 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 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 semiquantitative methods may include quantitative descriptions of frequency such as "having a frequency less than 10^{-2}/yr." 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 that can affect the event likelihood (reliability and availability qualities) are recognized as such and 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 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 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; 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 (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 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 (e.g., 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 in quantitative fashion 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 on 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 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 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 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 Chapter 3 of this NUREG 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.

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 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 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., 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 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 defense-in-depth is provided by IROFS that perform different safety functions 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, Section 5.4.3.4.4(7)(a) in Chapter 5 of this report 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:

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

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 to this NUREG, 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 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 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, the guidance of ISG-03, "Nuclear Criticality Safety Performance Requirements and Double Contingency Principle," issued February 2005, is applicable.

Use of Quantitative and Qualitative Information

Section 3.4.3.2(9) of Chapter 3 of this NUREG acknowledges that a mix of quantitative and qualitative information is often available to an analyst performing an ISA. The NUREG 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 to Chapter 3 of this NUREG).

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, etc. 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 10 CFR 70.61. 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 (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 them 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 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.

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

- 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; HazOp, fault tree, and other sophisticated methods may be appropriate for more complex or higher risk operations.

- In considering 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 ISG, 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 NUREG, 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. 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 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, 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 NUREG.

This guidance should be used to supplement NUREG-1718, "Standard Review Plan for the Review of an Application for a Mixed Oxide (MOX) Fuel Fabrication Facility," issued August 2000, Chapter 5, "Integrated Safety Analysis (ISA)," and Appendix A, "Example Procedure for Risk Evaluation."

References

U.S. Code of Federal Regulations, Title 10, 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

Field Code Changed

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, Section 70.61, "Performance Requirements," of the *Code of Federal Regulations* (10 CFR 70.61).

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," and this NUREG provide methods for reviewing integrated safety analyses (ISAs) by employing a semiquantitative risk index method. While one of these methods is used 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-11 in Appendix A to Chapter 3 of this report. 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, "Natural Phenomena Hazards," offers additional guidance regarding initiating probabilities from natural phenomena hazards.)

An initiating event does not have to be an IROFS failure. An item only becomes an IROFS if the ISA credits it for mitigation or prevention per the definition in 10 CFR 70.4. 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, 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

- 10 CFR 70.61, "Performance Requirements"
- 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. Initiating 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 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 NUREG 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 NUREG 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 those 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, Title 10*, Energy,* Part 70, "Domestic Licensing of Special Nuclear Material."

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

APPENDIX D

Field Code Changed

NATURAL PHENOMENA HAZARDS

Purpose

This appendix provides additional guidance addressing accident sequences that may result from natural phenomena hazards in the context of a license application or an amendment request under Title 10, Part 70, "Domestic Licensing of Special Nuclear Material," of the *Code of Federal Regulations* (10 CFR Part 70), Subpart H, "Additional Requirements for Certain Licensees Authorized To Possess a Critical Mass of Special Nuclear Material."

Introduction

This appendix provides additional guidance for reviewing the applicant's (or licensee's) evaluation of natural phenomena hazards up to and including "highly unlikely" events for both new and existing facilities.

Discussion

For facilities processing special nuclear materials, 10 CFR 70.61, "Performance Requirements," requires that individual accident sequences resulting in high consequences to workers and the public be "highly unlikely" and that sequences resulting in intermediate consequences to these receptors be "unlikely." Although the threshold levels that differentiate high-consequence events from intermediate-consequence events are established in the regulations, the definitions of "highly unlikely" and "unlikely" are not. According to 10 CFR 70.65(b)(9) and subject to staff approval, definitions of these terms must be included in the integrated safety analysis (ISA) summary submitted by applicants and licensees. Chapter 3 of this NUREG further describes the acceptance criteria for the definitions of these terms.

The implementation of these requirements may vary somewhat because of different definitions of likelihood proposed by different applicants (or licensees).[1] The regulation specifies quantitative consequence thresholds of the performance requirements (except for chemical releases). The regulation and its performance requirements pertain to existing facilities, as well as proposed facilities, and apply to manmade external hazards and natural phenomena hazards, in addition to process hazards. However, new facilities and new processes at existing facilities must also address the requirements of 10 CFR 70.64, "Requirements for New Facilities or New Processes at Existing Facilities," which includes the baseline design criterion for natural phenomena hazards (10 CFR 70.64(a)(2)). This baseline design criterion requires that "the design must provide for adequate protection against natural phenomena with consideration of the most severe documented historical events for the site." The Statement of Considerations (Reference 2) describes the application of the baseline design criteria as consistent with good engineering practice, which dictates that certain minimum requirements should be applied to design and safety considerations. The baseline design criteria must be applied to the design of

[1] For natural phenomena, deterministically defined events such as the probable maximum flood (PMF) or safe shutdown earthquake (SSE) which are used as reactor design bases can also be applied to 10 CFR Part 70 facilities as "highly unlikely" events. The actual probability (or likelihood) of such events may be difficult to define quantitatively and varies from site to site.

new facilities and new processes at existing facilities but does not require retrofits to existing facilities or existing processes (e.g., those housing or adjacent to the new processes). Also included in 10 CFR 70.64(b) are a requirement for incorporation of defense-in-depth in design and a requirement to prefer engineered controls over administrative controls.

New structures associated with facilities being reviewed, such as the gas centrifuge facilities and the mixed oxide fuel fabrication facility, will be designed and constructed to meet the seismic regulatory requirements. Hence, these facilities and additional new facilities to be licensed under 10 CFR Part 70 are not expected to present designs with seismic deficiencies. New facilities can also be expected to be sited above a "highly unlikely" flood such as the PMF and can be expected to withstand tornado winds and missiles, if necessary.

Most structures at existing nuclear fuel cycle facilities are built to a model building code, which includes meeting a design-basis earthquake having an exceedance probability of $2x10^{-3}$ per year to less than 10^{-3} per year (U.S. Department of Energy (DOE) Standard-1020-2002, Appendix C). Existing facilities are generally sited above the 100-year flood plain and are designed for wind as well as snow and ice loading as specified in applicable building codes. Extreme natural events such as "highly unlikely" floods and/or earthquakes have not been calculated for many existing sites, and it would be expensive and time consuming to do so.

The staff believes that many existing facilities can be shown to be in compliance with, or at least near compliance with, the performance requirements of the regulation by accounting for conservatisms in the seismic, flooding, and wind design of the facility. In addition, relatively minor engineered improvements and administrative measures may further enhance safety, at least with respect to the public and other offsite receptors.

Seismic Hazards

Potential damage to and/or failure of items relied on for safety (IROFS) as the result of ground movement and/or the seismic response of adjacent or interior IROFS must be considered in the ISA and ISA summary accident sequence evaluations. Damage or failures that also should be considered include the following:

- seismic-induced failure of a facility component which is not an IROFS but which can fall and damage an IROFS (for example, a heavy load drop from a crane onto a container)
- displacement of adjacent IROFS during a seismic event causing them to pound together
- displacement of adjacent components resulting in failure of connecting pipes or cables which may cause flooding, fires, and/or releases of radiological or chemical materials

Seismic event evaluations must also consider potential multiple failure of IROFS (for example, multiple failures of tanks).

DOE has also recognized the difference between earthquake design probability and the probability that a safety component cannot perform its function. To quantify this difference, DOE has developed a risk reduction factor, R, as the ratio between the seismic hazard exceedance probability and the performance goal probability. Conservatism in nuclear facility design arising from factors such as use of prescribed analysis methods, specification of material

strengths, and limits on inelastic behavior explains at least part of this apparent reduction in actual risk. Appendix C to DOE Standard-1020-2002 discusses this risk reduction factor.

For a consequence to affect the public or external site workers, licensed material or hazardous chemicals that could affect the safety of licensed material must be released through at least one, and often two, confinement barriers, such as the following:

- storage containers, glove boxes, tanks, or handling devices
- ventilation system dynamic confinement and filtration
- building structural shell

Criticalities, on the other hand, may result from the introduction of a moderator or loss of safe geometric control of confined materials.

By using risk reduction factors calculated for a facility and its specific components and/or estimating the degree of failure by comparison with the observed behavior of similarly constructed buildings during severe earthquakes, analysts can postulate reasonable scenarios. These scenarios may not release all the material at risk or present an unimpeded leak path to receptors. For example, some facilities might be able to show that, even in the case of an earthquake that is "highly unlikely," only certain types of containers or confinement systems are likely to be breached. If the amount of material contained in such containers is variable, then that probabilistic component may be factored into the overall likelihood of the accident sequence. If employing some of these mitigating considerations in the analysis requires reliance on special containers or procedures, then additional IROFS may also be needed. Another factor to consider is the likely rate of release based on the damage sustained. For example, some facilities may lose dynamic confinement but maintain building integrity. In some processes, radiologically and/or chemically hazardous material is held inside its primary containment at subatmospheric pressure. In these cases, even though the primary containments are inside a structure designed to withstand less than a "highly unlikely" earthquake, the subatmospheric conditions may be sufficient to limit both facility worker and offsite doses in the event of a greater earthquake. For example, an earthquake that results in limited subatmospheric containment losses may allow adequately trained workers to evacuate and/or take mitigative actions. The buildings containing cylinders of liquid uranium hexafluoride (UF_6) at gas centrifuge facilities are designed for a "highly unlikely" earthquake. In addition, some buildings at one of the proposed facilities are equipped with a seismically activated interlock (an IROFS) that will shut off the buildings' heating, ventilation, and air conditioning system during an event, thus limiting any leakage of UF_6 to the outside.

Flooding Hazards

Most fuel cycle licensees do not require large quantities of cooling water and, therefore, do not need to be located near large bodies of water. A site licensed under 10 CFR Part 70 does not need to meet prescriptive flood protection requirements but does have to meet the performance requirements for all credible events including flooding. A site meeting the flood protection requirements of a commercial reactor should be considered as being designed or located adequately to withstand a "highly unlikely" flooding event. Section 2.4 of NUREG-1407, "Procedural and Submittal Guidance for the Individual Plant Examination of External Events for Severe Accident Vulnerability," issued June 1991, states that the design-basis flood (which for river sites is the PMF) as described in Regulatory Guide 1.59, "Design Basis Flooding for Nuclear Power Plants," is estimated to have an exceedance frequency of less than 10^{-5} per year. Sites that do not meet this level of protection can still meet the 10 CFR 70.61 performance requirements but must be considered on an individual basis.

In evaluating the effects of flooding on existing facilities, the following flood-related hazards should be considered:

- river flooding
  - inundation and hydrostatic loading
  - dynamic forces
  - wave action
  - sedimentation and erosion
  - ice loading
- upstream dam failures
  - inundation and hydrostatic loading
  - dynamic forces
  - erosion and sedimentation
- precipitation/local storm runoff
  - inundation (local ponding) and hydrostatic loading
  - dynamic loads (flash flooding)
- tsunami, seiche, hurricane storm surge
  - Inundation and hydrostatic loading
  - dynamic forces
  - wave action

American National Standards Institute/American Nuclear Society Standard 2.8, "Determining Design Basis Flooding at Power Reactor Sites," describe methods for determining these flooding and water-related effects for reactor sites. These methods can be applied to 10 CFR 70.61 analyses with less conservatism in some of these parameters.

A standard siting requirement for residential and commercial developments is to be above the 100-year flood plain. For large river basins, warning time and time to secure materials and evacuate personnel will probably be available. For small streams, there may be relatively little warning in regard to thunderstorms and localized rainfall. In such cases, rapid actions may be the only administrative protection available. An evaluation of the effectiveness of proposed

protection will need to consider the effects of inundation, hydrostatic loading, erosion, and sedimentation. At a minimum, this would require that criticality events be prevented and materials remain confined within site structures.

At some sites, a delineation of the 500-year flood plain may also be available. If the site is above the 500-year flood plain, flooding may be considered an unlikely event[2] depending on the quality of the estimate. In this category, criticality events should still be prevented, but the breaching of a limited number of material containers may be allowable under the performance requirements (up to 25 rem for the public, up to 100 rem for workers, and a specified release limit) for events, that in terms of likelihood, are between "unlikely" and "highly unlikely."

In addition to the facility's location relative to the 100-year or 500-year flood plains, the effects of local intense precipitation and snow load should be considered. Local intense precipitation, especially in the form of snow, can result in roof collapse and localized site flooding. Normally, protection from local precipitation and snow is relatively easy to achieve through roof design and local site drainage design.

Wind and Tornado Loading

Wind design for an existing facility if prescribed by an applicable building code would have an annual exceedance probability of greater than or equal to $2x10^{-2}$. At such relatively high probabilities, tornado design criteria are not specified. However, depending on the geographic location of the facility, the effects of a tornado with an annual exceedance probability of 10^{-5} or greater may need to be considered.

Wind forces on walls of structures should be determined using appropriate pressure coefficients, gust factors, and other site-specific adjustments. If the wind is likely to blow inside the structure, either through design or wind-driven missile vulnerability, the effects of wind on internal IROFS requires consideration. If the winds are from a tornado, the effects of the atmospheric pressure change associated with the tornado must be considered. Normally, ventilation systems are most vulnerable to atmospheric pressure change, but windows, buried tanks, and sand filters can also be affected.

For straight winds, hurricanes, and weak tornadoes, missile criteria as specified in Table 3-3 of DOE Standard-1020-2002 may be considered. The missile specified is a 15-pound plank, measuring 2 inches by 4 inches, at a specified elevation and impact velocity. For facilities that may be subjected to more severe tornado missiles, the guidance in Tables 3-4 and 3-5 of DOE Standard-1020-2002 may be followed. For the tornado, a 3,000-pound automobile rolling and tumbling on the ground should also be considered. For such evaluations, the probability of the entire sequence should be considered, and missile criteria from either Table 3-4 or 3-5 of DOE Standard-1020-2002 may be used as appropriate.

Considerations for Existing Processes at Existing Facilities

[2] Even if the licensee defines "unlikely" as less than 10^{-3} per year for the process sequences in the ISA summary, the conservative assumptions inherent in most flood plain hydrologic studies, such as those performed for Federal Emergency Management Agency flood insurance rate maps, should justify the consideration of flooding above the 500-year flood plain as an unlikely event.

For existing processes at existing facilities, licensees are not required to address 10 CFR 70.64 baseline design criteria. They must still meet the performance requirements of 10 CFR 70.61, including accidents caused by natural phenomena, for which the staff may require additional IROFS to meet the performance requirements. Existing facilities can use IROFS in the form of additional administrative controls to meet the performance requirements without the need for design features normally required by accepted engineering practice. When near compliance can be obtained and complete compliance will be relatively costly, plants may request an exemption to the regulation.

As discussed earlier, many existing 10 CFR Part 70 facilities are not designed for an earthquake beyond that specified in applicable building codes. Although this design may provide fairly good seismic protection to the structure, it may not protect internal equipment. Also, an existing facility may not be designed to any specific seismic criteria in which case its ability to withstand earthquakes can only be estimated based on comparison with similar structures or through complex structural analysis. In such cases, licensees may add additional IROFS to meet the performance requirements. An example where such IROFS (procedures and upgrades) may be effectively implemented could be a facility where the consequences of a release of licensed material to the public in a seismic event would be from fires and/or explosions. In this case, fixes such as seismically qualified flammable gas shutoff valves or electrical shutoffs might provide a large decrease in potential seismic consequences.

In regard to flooding, flood elevations beyond that of the 100-year flood may not have been determined for the site. For sites in proximity to a river, these determinations could be expensive and time consuming. For these cases, flood warning time may allow measures such as moving material at risk and/or blocking doors and openings in the facility structure.

A facility's ability to withstand high winds, rain and snow loads, and exterior fires can likewise be improved through a combination of administrative procedures and engineered improvements. Removing material at risk from under walls or roofs that are not seismically designed can reduce potential releases in case of collapse from winds or roof loads.

Exemptions to the regulation may still be required for existing facilities even with administrative and engineered improvements. In regard to consequences to the public, complete compliance with 10 CFR 70.61 using realistic assumptions should be the goal if obtainable. Compliance with 10 CFR 70.61 regarding consequences to facility workers may require a request for an exemption once personnel protective equipment, emergency procedures, and worker training is accounted for. In evaluating a request for an exemption to the regulation, the expected operational life of the facility should also be factored into the determination of risk.

Considerations for New Processes at Existing Facilities

The design of new processes at existing facilities must address natural phenomena hazards in accordance with 10 CFR 70.64(a)(2), as well as the performance requirements of 10 CFR 70.61. Nevertheless, new processes at existing facilities may present the same problems in demonstrating compliance with 10 CFR 70.61 in regard to accident sequences initiated by natural phenomena as do existing facilities based on the design and/or siting of the original structures. In the case of new processes, the U.S. Nuclear Regulatory Commission staff should expect compliance with the performance requirements of 10 CFR 70.61 to the extent possible given the existing facility design and location. New processes at existing facilities also must meet the requirements of 10 CFR 70.64(b), which requires defense-in-depth and a preference for engineered controls over administrative controls. However, the staff cannot require structural improvements, permanent flood barriers, and other engineered improvements that could be considered retrofits to be applied to existing structures. New structural features within existing structures to prevent breaches in containment in the event of natural phenomena hazards may be considered, however. An example might be a seismically designed vault to hold radioactive materials associated with a new process. In regard to new processes, engineered controls, where feasible, are preferred over administrative procedures that might otherwise be proposed for an existing process with a limited operational lifetime. Such engineered improvements may not be required for licensing but could be scheduled to replace administrative procedures or other long-term compensatory measures on a timely basis after the start of operations. The objective is to encourage engineered safety in new processes compared to equivalent existing processes, while recognizing the restraints of the existing structures and location. Although primarily aimed at reducing risk to the public, the emphasis on engineered safety may also be applied to worker consequences in a way consistent with what has been accepted at other facilities.

Regulatory Basis

The regulation in 10 CFR 70.61 specifies performance requirements associated with risks identified by an ISA.

For new facilities or new processes at existing facilities, 10 CFR 70.64 specifies requirements, including baseline design criteria (a)(2), “Natural Phenomena Hazards.”

Technical Review Guidance

When examining the applicant’s evaluation of the effects of natural phenomena on its facility, reviewers should recognize that estimates of “unlikely” and “highly unlikely” natural phenomena such as the PMF or SSE may not exist for the particular site. Hence, extrapolation and/or transposition of extreme event estimates made for other relatively nearby facilities (such as power reactor sites) should be allowed where feasible and technically justifiable. In addition, sophisticated probabilistic tools such as Bayesian analysis or Monte Carlo sampling methods need not be employed to improve the estimate of likelihoods of natural phenomena event sequences unless desired by the applicant (or licensee). For the purpose of determining appropriate values of extreme events, deterministic events such as the PMF or SSE can be used in place of purely probabilistically determined “highly unlikely” events and may be preferable, depending on the quality of historical data. Where extreme events need to be coupled with other probability-driven mechanisms such as the release fraction or transport

pathway, already low likelihood combinations do not have to be made even less likely by the use of conservative parameters.

For existing facilities, due credit should be given to analysis assumptions and administrative controls, emergency procedures, and active engineered controls that do not change the design bases of the facility structures to natural phenomena. If the ISA and ISA summary demonstrate that the existing facility is near compliance (within an order of magnitude of a likelihood threshold or within 50 percent of meeting a consequence threshold, but not both), an exemption to the regulation may be considered.

An example evaluation for an amendment request is provided in the annex to this appendix.

Recommendation

This guidance should be used to supplement Chapter 3 of this NUREG.

References

American National Standard Institute/American Nuclear Society (ANSI/ANS), ANS-2.8, "Determining Design Basis Flooding at Power Reactor Sites," July 1992.

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

U.S. Department of Energy, DOE-Standard-1020-2002, "Natural Phenomena Hazards Design and Evaluation Criteria for Department of Energy Facilities," 2002.

U.S. Nuclear Regulatory Commission, "Domestic Licensing of Special Nuclear Material; Possession of a Critical Mass of Special Nuclear Material," *Federal Register*, Vol. 65, No. 181, pp. 56211–562331, September 18, 2000.

U.S. Nuclear Regulatory Commission, "Procedural and Submittal Guidance for the Individual Plant Examination of External Events (IPEEE) for Severe Accident Vulnerabilities," NUREG-1407, June 1991.

U.S. Nuclear Regulatory Commission, Regulatory Guide 1.59, "Design Basis Flooding for Nuclear Power Plants," Revision 2, August 1997.

ANNEX TO APPENDIX D

EXAMPLE OF NATURAL PHENOMENA HAZARD REVIEW FOR COMPLIANCE WITH 10 CFR 70.61

This example review is for an amendment to authorize operations in a blended low-enriched uranium oxide conversion building (OCB). The site is located near a river and is just above the 100-year flood plain of a nearby creek. The Effluent Process Building (EPB) was also part of the amendment but was not evaluated because the quantities of radioactive material or hazardous chemicals (that come under U.S. Nuclear Regulatory Commission (NRC) regulation) contained in the EPB are not considered sufficient to exceed the consequence threshold for "unlikely" events given in Title 10, Section 70.61, "Performance Requirements," of the *Code of Federal Regulations* (10 CFR 70.61).

Seismic Evaluation

The OCB is of reinforced concrete construction and is constructed to seismic criteria contained in the Standard Building Code (SBC-1999) which is equivalent to being designed for an earthquake with a probability of exceedance of approximately $4x10^{-4}$ per year. Using Appendix C to DOE-STD-1020-2002, the NRC staff determined the risk reduction factor to be 4, which gives the structure a likelihood of significant damage from an earthquake of 10^{-4} per year or less. Hence, the collapse or loss of building integrity from an earthquake may be considered to be "highly unlikely" as the probabilistic value of "highly unlikely" indicated by the applicant was a probability of exceedance of 10^{-4} to 10^{-5} per year. Within the building, the material at risk consists of low-enriched uranyl nitrate liquid, ammonium diuranate slurry, and uranium dioxide powder. All of these materials are expected to be within containers, and spillage during a seismic event is expected to be minimal. Since the building is expected to retain its integrity, the leak path factor will be relatively low even without dynamic confinement from the ventilation system. Facility workers are expected to take actions to limit personal intake of radionuclides. The staff concludes that the OCB complies with the performance requirements of 10 CFR 70.61 with regard to seismic events.

High Winds Evaluation

The OCB structure is also designed for wind loads in accordance with the SBC-1999, and the probability of a tornado impacting the facility is less than 10^{-5} per year. Therefore, the facility needs to be evaluated only in regard to the effects of wind loads and missiles, but not for tornadoes. The NRC staff considers the reinforced concrete exterior walls of the OCB to be adequate to withstand high wind velocities as well as missiles (from DOE-STD-1020-2002) that should be assumed for such events. The staff considers a collapse of building walls because of wind forces such that radioactive material would escape to be "highly unlikely." In addition, the meteorological conditions likely to result in severe winds may be forecast in advance and protective measures taken. The staff concludes that the OCB complies with the performance requirements of 10 CFR 70.61 with regard to wind events.

Flooding Evaluation

The lowest floor in the OCB is 15 feet above the 100-year flood from an adjacent creek. From a review of the topography of the site area, it appears that flooding of the site could occur, most likely from flooding of the nearby river with coincident flooding of the adjacent creek which could back up through the railroad culvert. This event is expected to have warning time and may overtop the railroad embankment to the north of the facility and flood parts of the nearby town. However, the facility is sufficiently removed from the main channel of the river that flood-induced scouring and erosion would not be expected. In addition, the hydrostatic loading from the flood on the exterior walls of the OCB would not be expected to cause collapse. The primary concern is inundation which could float unsecured containers within the OCB but not remove them from the facility. A criticality event cannot be excluded, but could occur only in the flooded and, therefore, evacuated section of the plant and would not affect facility workers. In addition, the warning time would allow the movement of material to reduce the likelihood of a flood-induced criticality. The staff concludes that the OCB complies with the performance requirements of 10 CFR 70.61 with regard to flooding.

APPENDIX E

HUMAN FACTORS ENGINEERING FOR PERSONNEL ACTIVITIES

The purpose of this review is to establish that human factors engineering (HFE) is applied to personnel activities identified as safety-significant, consistent with the findings of the integrated safety analysis (ISA), and the determination of whether an item relied on for safety has special or unique safety significance. A graded approach commensurate with the complexity and integration and operation of the control systems is appropriate. The application of HFE to personnel activities ensures that the potential for human error in the facility operations was addressed during the design of the facility by facilitating correct, and inhibiting wrong, decisions by personnel and by providing means for detecting and correcting or compensating for error.

10 CFR 70.61(e) requires a safety program to ensure that each item relied on for safety will be available and reliable to perform its intended function when needed. Therefore the applicant should identify those "personnel activities"[2] that are considered IROFS and personnel activities that support safety (e.g. maintenance). A HFE review should be performed to demonstrate compliance with 70.61(e). Also, the applicant should demonstrate how personnel activities will enhance safety by reducing challenges to IROFS as required in 10 CFR 70.64(b)(2).

The human factor review should be conducted by a human factor specialist and an ISA reviewer. The review should also be coordinated with the reviewers of other technical areas and the reviewer of management measures as necessary.

AREAS OF REVIEW & ACCEPTANCE CRITERIA

Some facilities rely heavily on automated systems employing advanced digital instrumentation and control technology. These systems may be complex, with potential negative impacts on human performance activities in both operations and maintenance. The scope of review for the HFE for personnel activities should be consistent with the results of the ISA and include, as appropriate[3]:

A. Identification of Personnel Activities—The applicant should appropriately identify the personnel activities such that the reviewer can understand the actions, the human systems interfaces (HSI) involved, and the consequences.

B. HFE Design Review Planning—The applicant's approach for planning HFE design review should include:

   i. Identification of appropriate goals and scope to ensure that HFE practices and guidelines are implemented during design, construction, and operation of the facility.

Formatted: Bullets and Numbering

Formatted: Bullets and Numbering

[2] For the purposes of this chapter, the phrase "personnel activities" represents personnel activities identified as items relied on for safety (IROFS) and personnel activities that support safety, such as maintenance.

[3] All nine areas of review (A-I) may not be necessary for a specific application. Areas of review should be based on the applicant's provisions to address personnel activities consistent with the ISA findings; the similarity of the associated HFE issues for similar type plants; and the determination of whether an item relied on for safety has special or unique safety significance.

ii. Implementation by an HFE team that has the appropriate composition, experience, and organizational authority to ensure that HFE is considered in the design of HSI for personnel activities. The HFE team's responsibilities include ensuring the proper development, execution, oversight, and documentation of the HFE function. Depending on the identification of personnel activities, it may be appropriate for the HFE team to consist of a single individual.

iii. An HFE team that attains the HFE goals and scope through established processes and procedures and that tracks HFE issues. An HFE function that ensures that all aspects of the personnel activities including the HSI are developed, designed, and evaluated on the basis of a structured approach using HFE.

C. Operating Experience Review (OER)—to the extent possible the applicant should identify safety-related HFE events or potential events that have occurred in existing facilities that are similar to the proposed facility. The applicant should:

i. Review the HFE-related events or potential events for relevance;

ii. Analyze the HSI technology employed for the relevant HFE events or potential events; and

iii. Conduct (or review existing) operator interviews and surveys on the HSI technology for the relevant HFE events or potential events.

D. Functional Allocation Analysis and Task Analysis

i. Functional allocation analysis: The functional allocation analysis should be based on the OER. Personnel activities should be functionally allocated to take advantage of human strengths and to avoid demands that are not compatible with human capabilities.

ii. Task analysis: The task analysis should include the task analysis scope, identification and analysis of critical tasks; detailed description of personnel demands (e.g., input, processing, and output); iterative nature of the analysis; and incorporation of job design issues. The task analysis should address each operating mode for each personnel activity (e.g., startup, normal operations, emergency operations, and shutdown). The task analysis results support the functional allocation.

E. HSI Design, Inventory, and Characterization

The HSI design should incorporate the functional allocation analysis and task analysis into the detailed design of safety-significant HSI components (e.g., alarms, displays, controls, and operator aids) through the systematic application of HFE. The HSI design should include the overall work environment, the work space layout (e.g., control room and remote shutdown facility layouts), the control panel and console design, the control and display device layout, and information and control interface design details. The HSI design process should ensure the application of HFE to the HSI required to perform personnel activities. The HSI design process should exclude the development of extraneous controls and displays. The HSI design documentation should include a complete HSI inventory and the basis for the HSI characterization.

Formatted: Bullets and Numbering

Formatted: Bullets and Numbering

Formatted: Bullets and Numbering

Formatted: Bullets and Numbering

F. Staffing—Staffing should be based on a review of the number and qualifications of personnel for each personnel activity during all plant operating conditions. The applicant should conduct this review in a systematic manner that incorporates the functional allocation and task analysis results.

Categories of personnel should be based on the types of personnel activities. Staffing considerations should include issues identified in the OER, functional allocation, HSI design, procedure development, and V&V.

G. Procedure Development—The applicant's procedure development for personnel activities should incorporates HFE principles and criteria, along with all other design requirements, to develop procedures that are technically accurate, comprehensive, explicit, easy to utilize, and validated consistent with the acceptance criteria in Section 15.5.4 of this SRP. Because procedures are considered an essential component of the HSI design, they should be derived from the same design process and analyses as the other components of the HSI (for example, displays, controls, operator aids) and subject to the same evaluation processes. Procedures to support the personnel activity might include: generic technical guidance, plant and system operations, abnormal and emergency operations, tests (for example, preoperational, startup, and surveillance), and alarm response.

H. Training Program Development—the applicant's training program development should addresses all personnel activities. The training program development indicates how the knowledge and skill requirements of personnel will be evaluated, how the training program development is coordinated with the other activities of the HFE design process, and how the training program will be implemented in an effective manner consistent with human factors principles and practices.

The training program development should address the areas of review and acceptance criteria described in Chapter 11 of this SRP and should result in a training program that provides personnel with the qualifications commensurate with the personnel activities.

I. Verification & Validation (V&V)—V&V confirms that the design incorporates HFE to HSI in a manner that enables the successful completion of personnel activities. The V&V should be applied to personnel activities (see Item A) and HSI design (see Item E). The V&V process should consist of the following:

i. HSI task support verification: HSI components should be appropriately provided for personnel activities through HSI task support verification. The verification should show that each HSI identified the task analysis (see Item D(ii)) and that the HSI design (see Item E) are appropriately provided, yet minimizes the incorporation of information, displays, controls, and decorative features that unnecessarily complicate personnel activities.

ii. HFE design verification: The HFE design verification should show that each HSI identified for a personnel activity incorporated HFE into the design. Deviations from accepted HFE principles and guidelines should be justified or documented for resolution/correction. If all HSI components are not addressed by HFE design verification, then an alternative multidimensional sampling methodology should be used to assure comprehensive consideration of the safety significance of HSI components. The sample size should be sufficient to identify a range of significant safety issues.

Formatted: Bullets and Numbering

Formatted: Bullets and Numbering

i. Integrated system validation: The applicant should perform a performance-based evaluation of the integrated design to ensure that the HFE/HSI supports safe operation of the plant. Integrated system validation is performed after HFE problems identified in HFE design activities are resolved or corrected because these may negatively affect performance and, therefore, validation results. Validation is performed by evaluating personnel activities using appropriate measurement tools. All personnel activities should be tested and found to be adequately supported in the design, including personnel activities outside the control room. Human factors issue resolution verification: The applicant should verify that HFE issues identified during the design process were addressed and resolved. Issue resolution verification should be documented in the HFE issue tracking system established by the HFE team (see Item B). Issues that cannot be resolved until the HSI design is constructed, installed, and tested should be identified and incorporated into the final HFE/HSI design verification.

Formatted: Bullets and Numbering

ii. Final HFE/HSI design verification: The applicant should commit to performing a final HFE/HSI design verification if the applicant cannot demonstrate that it has fully evaluated the actual installation of the final HSI design in the plant through the V&V activities described above. Final HFE/HSI design verification should demonstrate that in-plant **HFE** design implementation conforms to the HFE design (see Item E) as modified V&V activities. V&V activities should be performed in the order listed above, as necessary. However, the applicant may find that it is necessary to iterate in order to address design corrections and modifications that occur during V&V.

Formatted: Bullets and Numbering

REFERENCES

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

NUREG-1718, "Standard Review Plan for the Review of a License Application for a Mixed Oxide Fuel Fabrication Facility" NRC: Washington, D.C. 2000.