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 μ = 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,

Formatted: Spanish (Puerto Rico)
Formatted: Spanish (Puerto Rico)
Formatted: Spanish (Puerto Rico)
Formatted: Spanish (Puerto Rico)
Formatted: Spanish (Puerto Rico)
Formatted: Spanish (Puerto Rico)
Formatted: Spanish (Puerto Rico)
Formatted: French (France)
Formatted: French (France)
Formatted: French (France)
Formatted: French (France)
Formatted: French (France)
Formatted: French (France)
Formatted: French (France)
Formatted: French (France)

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.