APPENDIX A

EXAMPLE PROCEDURE FOR ACCIDENT SEQUENCE EVALUATION

The appendix provides the NRC reviewer with a method for reviewing integrated safety analyses (ISAs). For the applicant, this appendix outlines one approach for performing ISA analyses of process accident sequences. 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 10 CFR 70.61 and, therefore, require designation of items relied on for safety (IROFS) and supporting management measures. Descriptions of these general types of higher consequence accident sequences need to be reported in the ISA Summary.

This appendix works through 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 quantitative information to be considered, if available. 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 requiring 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 of this appendix describes 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 the 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, what engineered or administrative IROFS 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

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.” These 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 forecast 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 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
Note: > = greater than, < = less than, and ≤ = less than or equal to

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	“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. The risk index matrix, along with computed risk index values, is illustrated in Table A-3. The shaded blocks identify accidents of which the consequences and likelihoods yield an unacceptable risk index and for 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 4 means the accident sequence is acceptably protected 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 this chapter in Subsections 5 and 7 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 to 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
Note: > = greater than, < = less than, and ≤ = less than or equal to

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, 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.

Quantitative measures of likelihood are based on the NRC's determinations reported in Item 9 of Section 3.4.3.2 of SRP Chapter 3: “highly unlikely” means a frequency of less than 10^{-5} per-event per-year, and “unlikely” means a frequency within the range of 10^{-4} and

10^{-5} per-event per-year. The numerical scores assigned to each likelihood of occurrence are presented in Table A-6.

Table A-6: Event Likelihood

	Likelihood Category	Probability of Occurrence*
Not Unlikely	3	more than 10^{-4} per-event per-year
Unlikely	2	between 10^{-4} and 10^{-5} per-event per-year
Highly Unlikely	1	less than 10^{-5} per-event per-year

*Based on approximate order-of-magnitude ranges

In assessing the adequacy of engineered and administrative IROFS, individual accident frequencies greater than 10^{-5} per-year may not be evaluated as “highly unlikely.” Similarly, accident sequences having frequencies more than 10^{-4} per-year may not be considered as “unlikely.”

The accident evaluation method described below does not preclude the need to comply with the double-contingency principle for sequences leading to criticality. Although exceptions are permitted with compensatory measures, double contingency should, in general, be applied. Double contingency is needed as there are usually insufficient firm data as to the reliability of the IROFS equipment and administrative IROFS procedures used in criticality safety. If only one item were relied on to prevent a criticality, and it proved to be less reliable than expected, then the first time it failed, a criticality accident could result. For this reason, at least two independent IROFS should be used. Inadequate IROFS can then be determined by observing their failures without also suffering the consequences of a criticality accident. Even with double contingency, each IROFS should be sufficiently unlikely to fail, for if one of the two items that establish double contingency is actually ineffective, criticality will still be unlikely.

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.

A.5 RISK INDEX EVALUATION SUMMARY

As previously mentioned, an 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. The risk index calculation is summarized below.

Accident sequences result from initiating events, followed by failure of one or more IROFS. Thus, in Table A-7 there are columns for the initiating event and for IROFS. IROFS may be mitigative or preventive. Mitigative IROFS are measures that reduce the consequences of an accident. The phrase “uncontrolled and/or unmitigated consequences” describes the results when the system of preventive IROFS fails and mitigation also fails. Mitigated consequences result when the preventive IROFS fail, but mitigative measures succeed. These are abbreviated in the table as “unmit.” and “mitig.,” respectively. Index numbers are assigned to initiating events, IROFS failure events, and mitigation failure events, based on the reliability characteristics of these items.

With redundant IROFS and in certain other cases, there are sequences in which an initiating event places the system in a vulnerable state. While the system is in this vulnerable state, an IROFS must fail for the accident to result. Thus, the frequency of the accident depends on 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, depending on the number of events involved, are added to obtain a total likelihood index, T. 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 and certain IROFS failures. When failure *probabilities* are required for an event, Table A-10 provides the index values. Table A-11 provides index numbers *for durations* of failure. These are used in certain accident sequences where two IROFS must simultaneously be in a failed state. In this case, one of the two controlled parameters will fail first. It is then necessary to consider the duration that the system remains vulnerable to failure of the second. This period of vulnerability can be terminated in several ways. The first failure may be “fail-safe” or be continuously monitored, thus alerting the operator when it fails so that the system may be quickly placed in a safe state. Or the IROFS may be subject to periodic surveillance tests for hidden failures. When hidden failures are possible, these surveillance intervals limit the duration that the system is in a vulnerable state. The reverse sequences, where the second IROFS fails first, should be considered as a separate accident sequence. This is necessary because the failure frequency and the duration of outage of the first and the second IROFS may differ. The values of these duration indices are not merely judgmental. They are directly related to the time intervals used for surveillance and the time needed to render the system safe.

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	Initiating Event (a)	Preventive Safety Parameter 1 or IROFS 1 Failure/Success (b)	Preventive Safety Parameter 2 or IROFS 2 Failure/Success (c)	Mitigation IROFS Failure/ Success (d)	Likelihood* Index T uncontrolled/ controlled (e)	Likelihood Category (f)	Consequence Evaluation Reference	Consequence Category (g)	Risk Index (h=f x g) uncontrolled/ controlled (h)	Comments & Recommendations
PPB2-1A (Criticality from blender leak of UO_2)	See IROFS 1 (Note 1)	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	Unc T = -1 Con T = -7	Unc 3 Con I	Rad 35	3 (Crit: 3, rad: 0)	9 3	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)	Blender leaks UO_2 Frqi = -1	PPB2-C1: Mass Control Success: leaked UO_2 below critical mass	PPB2-C2: Moderation Success: no moderator	Ventilation Failure: Ventilated blender enclosure Prf = -3	Unc T = -1 Con T = -4 Con T = -1	Unc 3 Unmit 2 Mitig 3	Rad 36	Unc 2 Unmit 2 Mitig 1	6 Unmit 4 Mitig 3	Rad consequences, no criticality unmitigated sequence: IROFS 1 & mitigation fail. T= -1-3 = -4 Mitig: IROFS 1 fails, mitig IROFS does not fail. T = -1
PPB2-1C	See IROFS 1 (Note 1)	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 = -2	N/A	Unc T = -2 Con T = -6	Unc 2 Con 1	Rad 35	3 (Crit: 3, rad: 0)	6 3	Criticality by reverse sequence of PPB2-1A. Moderation fails first. Note different likelihood. T = -6
PPB2-2	Fire in Blender Room Frqi = -2	Fire Suppression Failure: Fails on demand: Prf1 = -2	N/A	N/A	Unc T = -2 Con T = -4	Unc 2 Con 2	Rad 37	2 (rad) 1	4 2	Event sequence is just initiating event plus one IROFS failure on demand

*Likelihood index T is a sum; uncontrolled: T=frqi or frq1; controlled: includes all indices T=a+b+c+d.

Note 1: For these sequences the initiating event is failure of one of the IROFS, hence the frequency is assigned under that IROFS.

Table A-8: Determination of Likelihood Category

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

*The likelihood category is determined by calculating the likelihood index, T, then using this table. The term T is calculated as the sum of the indices for the events in the accident sequence.

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 can be 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.
** The index value assigned to an IROFS of a given type in column 3 may be one value higher or lower than the value given in column 1. Criteria justifying assignment of the lower (more negative) value should be given in the narrative describing ISA methods. Exceptions require individual justification.

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.)	Can 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 is accounted for in establishing the overall likelihood that an accident sequence will continue to the defined consequence. Thus, the time to discover and repair the failure is accounted for in establishing the risk of the postulated accident. Accordingly, as long as the actual undiscovered failures and repair times in service are conservatively described by the applicant's chosen duration of failure index and as long as the defined risks (reported in the ISA Summary) associated with the consequences are acceptable pursuant to 10 CFR 70.61, then such failures do not imply a violation of the approved license.

For all these index numbers, the more negative the number is the less likely the failure. 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.

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. The consequence category is chosen for the most severe consequence.

As shown in the first row of Table A-7, the failure duration index can make a large contribution to the total likelihood index. Therefore, the reviewer should verify that there is adequate justification that the failure will be corrected in the time ascribed to the duration index. In general, duration indices with values less than minus one (-1), corresponding to 36 days, should be based on intentional monitoring of the process. The duration of failure for an unmonitored process should be conservatively estimated.

Table A-7 provides two risk indices for each accident sequence to permit evaluation of the risk significance of the IROFS involved. To measure whether an IROFS has high risk significance, the table provides an “uncontrolled risk index,” determined by modeling the sequence with all IROFS as failed (i.e., not contributing to a lower likelihood). In addition, a “controlled risk index” is also calculated, taking credit for the low likelihood and duration of IROFS failures. When an accident sequence has an uncontrolled risk index exceeding 4 but a controlled index of less than 4, the IROFS involved have a high risk significance because they are relied on to achieve acceptable safety performance. Thus, use of these indices permits evaluation of the possible benefit of improving IROFS and also whether a relaxation may be acceptable.

Table A-12 provides a more detailed description of the accident sequences used in the example of Table A-7. The reviewer needs the information in Table A-12 to understand the nature of the accident sequences listed in Table A-7. Table A-7 lacks room to explain any but the simplest failure events.

Table A-13 explains the IROFS and external initiating events that appear in the accident sequences in Table A-7. The reviewer needs the information in Table A-13 to understand why the initiating events and IROFS listed in Table A-7 have the low likelihood indices assigned. Thus, Table A-13 should 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. Table A-13 must also justify why external events, which are not obviously extremely unlikely, have the low likelihoods that are being relied on for safety. The applicant should provide *separate* tables to list the IROFS for criticality, chemical, fire, radiological, and environmental accidents. If an applicant chooses to classify IROFS by applying different levels or grades of quality assurance, then the applicant should also provide the appropriate quality assurance grade for the IROFS.

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.
PPB2-2	Initiating event is a fire in the blender room. Fire is not extinguished in time. UO_2 is released from process equipment. Offsite dose estimated to exceed 1 mSv (100 mrem).

Table A-13: Descriptive List of Items Relied on for Safety

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 engineered IROFS, 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 ACCIDENT SUMMARY AND RISK INDEX ASSIGNMENT FOR TABLE A-7

The definitions for the contents of each column in the accident summary tabulation, Table A-7, are provided below.

Accident Identifier
This column identifies the accident sequence being analyzed. The ISA will have all accident sequences for uniquely identified facility processes, referred to here as "nodes." Symbols, names, or numbers of these nodes permit them to be uniquely identified. For example, the "blender hopper" node described in Table A-7 has the unique identifying symbol PPB2. PPB2-1is the first accident sequence identified in that node. By reviewing example accident sequences presented in the ISA Summary and the selected accident sequences contained in the ISA, the reviewer(s) can evaluate and confirm (1) the adequacy of the IROFS for preventing accidents, and (2) the bases for making the consequence and likelihood assignments in the table.

Initiating Event (Column a)
This column lists initiating events or IROFS failures that are typically identified in the PHA phase of the ISA and that may lead to consequences exceeding those identified in 10 CFR 70.61. Initiating events are of several distinct types: (1) external events, such as hurricanes and earthquakes; (2) facility events external to the node being analyzed (e.g., fires, explosions, failures of other equipment, flooding from facility water sources); (3) deviations from normal operations of the process in the node (i.e., credible abnormal events); and (4) failures of IROFS of the node. The tabulated initiating events should only consist of those that involve an actual or threatened failure of IROFS or that cause a demand requiring IROFS to function to prevent consequences exceeding 10 CFR 70.61 levels. The frequency index number for initiating events is referred to in the table by the symbol "frqi." Table A-9 provides criteria for assigning a value to frqi. Usually, there is insufficient room in a tabular presentation like Table A-7 to describe events accurately. Consequently, the applicant should provide supplementary narrative information to adequately describe each general type of accident sequence in Table A-7. Cross-referencing between this information and the table should be adequate (e.g., the unique symbolic accident sequence identifiers can be used). Table A-12 is an example of a list of supplementary accident sequence descriptions corresponding to Table A-7.

Preventive IROFS 1 Failure/Success (Column b)
This column addresses the failure or success of the safety parameter designated to prevent consequences exceeding 10 CFR 70.61 levels. Specific IROFS that may be needed to maintain the safety parameter should be included in this table. If separate parameters or IROFS are used to prevent different consequences, separate rows in the table should be defined corresponding to each type of consequence. Table A-7 contains an example of a set of related sequences so separated. Accident sequences where two IROFS must simultaneously be in a failed state require assignment of three index numbers (1) the failure frequency of the first IROFS, frq1, (2) the duration of this failure, dur1, and (3) the failure frequency of the second IROFS, frq2. For such accident sequences, the initiating event is failure of the first IROFS. In these cases, frq1 is assigned using Table A-9. The failure duration of the first IROFS is assigned using Table A-11. Other accident sequences may be more easily described as a failure of the IROFS on demand after the occurrence of an initiating event. In these cases, the failure probability index number, prf1, is assigned using Table A-10.

Preventive IROFS 2 Failure/Success (Column c)

This column is provided in case a second preventive IROFS is designated. The failure frequency or failure probability on demand is assigned in the same manner as for preventive IROFS 1.

Mitigation IROFS Failure/Success (Column d)
This column is provided in case IROFS are available to mitigate the consequences of the accident sequence. That is, they reduce, but do not eliminate, the consequences of an accident sequence. An IROFS that eliminates all adverse consequences should be considered preventive.

Likelihood Index (Column e) and Likelihood Category (Column f)
This column lists the likelihood category number for the risk matrix, which is based on the total likelihood index for an accident sequence. The total likelihood index, T, is the sum of the indices for those events that comprise an accident sequence which normally consists of the initiating event and failure of one or more IROFS, including any failure duration indices. However, accident sequences may consist of varying numbers and types of undesired events. Methods for deciding what frequencies and failure durations need to be considered will be described later in this appendix. Based on the sum of these indices, the likelihood category number for the risk matrix is assigned using Table A-8.

Consequence Evaluation Reference
This column permits identification of the consequence calculations that relate to this accident sequence. Multiple references may be required to refer to calculations of the different types of consequences (e.g., radiological, chemical, etc.).

Consequence Category (Column g)
This column is provided to assign the consequence category numbers from the risk matrix based on estimating the consequences of all types (i.e., radiological, criticality, chemical, and environmental) of accident sequences that may occur. Accident sequences having IROFS to mitigate consequences must be divided into two cases, one where the mitigation succeeds, and one where it fails, each with different consequences. The two cases may be tabulated in one row of Table A-7, but the mitigated and unmitigated consequences should be separately indicated. Unless the mitigated case results in consequences below those levels identified in 10 CFR 70.61, both cases must satisfy the likelihood requirements as shown by the risk matrix.

Risk Index (Column h)
This column is provided to list the risk index, which is calculated as the product of the likelihood category and consequence category numbers. This is shown in the column heading by the formula “h = f x g.” Sequences with values of h less than or equal to 4 are acceptable. Another risk index can also be calculated as the product of the consequence category number times the likelihood category associated with only the failure frequency index for the initiating event. The resulting product can be referred to as the “unmitigated” risk index. It is unmitigated in the sense that no credit is taken for the functioning of any subsequent IROFS. For example, in the first three cases in Table A-7, the initiating event is failure of preventive IROFS 1. In these cases, the failure frequency of preventive IROFS 1 is used to determine the likelihood category when calculating the unmitigated risk index.

Comments and Recommendations
This column records ISA team recommendations. It is especially useful when the existing system of IROFS is evaluated as being deficient. This may happen because a newly identified

accident sequence is not addressed by existing IROFS or because an unacceptable performance deficiency has been found in the existing IROFS.

A.7 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.8 DETERMINATION OF FAILURE FREQUENCY INDEX NUMBERS IN TABLE A-9

Table A-9 is used to assign frequency index numbers to plant initiating events and IROFS failures as found in the columns of Table A-7. The term "failure" must be understood to mean not merely failure of the IROFS but also a violation of the process safety. In the example in Table A-7, accident sequence PPB2-1A involves loss of mass control over uranium dioxide (UO_2) in a blender. If criticality is the concern, failure does not occur unless UO_2 accumulates to a critical mass before the leak is stopped. For radiological consequences, any amount leaked may cause exposure. In assessing the frequency index, this factor should be considered because many IROFS failures do not cause safety limits to be exceeded.

Table A-9 provides two columns with two sets of criteria for assigning an index value, one based on type of IROFS, the other on observed failure frequencies. Since IROFS of a given type have a wide range of failure frequencies, assignment of index values based on this table should be done with caution. Due consideration should be given to whether the IROFS will actually achieve the corresponding failure frequency in the next column. Based on operational experience, more refined criteria for judging failure frequencies may be developed by an individual applicant. In the column labeled "Based on Type of IROFS," references to redundancy allow for IROFS that may themselves have internal redundancy to achieve a necessary level of reliability.

Another objective basis for assignment of an index value is actual observations of failure events. These actual events may have occurred in the applicant's facility or in a comparable process elsewhere. Justification for specific assignments may be noted in the Comments column of Table A-7.

As previously noted, the definition of "failure" of an IROFS to be used in assigning indices is, for nonredundant IROFS, a failure severe enough to cause an accident with consequences exceeding those of 10 CFR 70.61. For redundant IROFS, it is a failure such that, if no credit is taken for functionality of the IROFS, an accident with consequences exceeding the performance requirements of 10 CFR 70.61 could result. If most IROFS malfunctions qualify as such failures, the index assignments of this table are appropriate. If true failure is substantially less frequent, credit should be taken and adequate justification provided.

Note that indices less than (more negative than) -1 should not be assigned to IROFS unless the configuration management, auditing, and other required management measures are of high quality, because, without these measures, the IROFS may be changed or inadequately maintained. The reviewer should be able to determine this from the tabular summary of IROFS provided in the application. This summary should identify the process parameters to be controlled and their safety limits and include a thorough description of the IROFS and the applied management measures.

A.9 DETERMINATION OF 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.10 DETERMINING 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 upon to meet the performance requirements of 10 CFR 70.61. The reviewer(s) examine 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). The types of management measures are maintenance, training, configuration management, audits and assessments, quality assurance, etc. Certain 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 meeting all the provisions of these chapters have acceptable management measures. IROFS may, with justification, have lesser management measures than those described. However, every IROFS in accident sequences leading to Consequence Categories 2 or 3 should be assigned at least a minimal set of management measures. Specifically, to defend against common mode failure of all IROFS on a process, this minimal set of measures must include (a) adequate configuration management, (b) regular auditing for the continued effectiveness of the IROFS, (c) adequate labeling, training, or written procedures to ensure that the operating staff is aware of the safety function, (d) adequate surveillance and corrective maintenance, and (e) adequate preventive maintenance.

If lesser or graded management measures are applied to some IROFS, Tables A-7 and A-13 and the narratives associated with them must identify to which IROFS these lesser measures are applied. In addition, information indicating that acceptable reliability can be achieved with these lesser measures must be presented. The specifics of how each management measure, such as the surveillance interval, type of maintenance, or type of testing, is applied to each IROFS need not be provided, for the NRC recognizes that such specific measures must be applied differently to each IROFS to achieve adequate reliability. The formality, documentation, and quality assurance requirements applied to these direct management measures that may be graded generically in a risk-informed manner must be documented.

The following paragraphs describe the application of management measures to IROFS based on the risk importance of the item in an accident sequence, as defined by (1) the uncontrolled risk index shown in Table A-7, and (2) the accident likelihood index, T, also described in Table A-7:

- For a particular accident sequence that would have unmitigated consequences in the two highest categories identified in 10 CFR 70.61, IROFS should reduce the risk from initially high risk (an uncontrolled risk index of 6 or 9 from Table A-3) to an acceptable risk (controlled risk index of less than or equal to 4).

- For those sequences that are initially evaluated as being in an acceptable risk category (an uncontrolled risk index of less than or equal to 4), a more detailed discussion is necessary. Some such accidents could have a relatively high uncontrolled likelihood (see discussion under B below), yet be of low consequence so that the risk is acceptable without IROFS. However, if the accident consequence of interest is a nuclear criticality, the accident's likelihood must be "highly unlikely," irrespective of the expected magnitude of consequence. Further, for accident sequences resulting in nuclear criticality, double contingency should be achieved, thus requiring at least one more IROFS and an initiating event of low probability. With this exception for criticality sequences, the following three cases apply:

  A. If the initiating event is *not* an IROFS failure, assurances for IROFS are not necessary. No additional risk reduction is required. However, for accident sequences claimed to be highly unlikely, the assessment that the initiating event has such a low probability must be adequately justified in the application.

  B. If the initiating event *is* an IROFS failure, and if the likelihood of that failure is taken to be more than a few times per facility lifetime (T is greater than -2), assurances for that IROFS may be less. Any subsequent IROFS in the accident sequence will be unregulated.

  The rationale is that since T is greater than -2, the likelihood category is 3. Therefore, the consequence category should not be greater than 1, to limit the uncontrolled risk index to, at most, 4. As the consequence category is low, the assurance level can be reduced.

  C. If the initiating event *is* an IROFS failure, and if the likelihood of that failure is taken to be *less* than a few times per facility lifetime (T is less than or equal to -2), assurance for this IROFS must satisfy the full baseline design requirements. No regulation of subsequent IROFS in the sequence is necessary.

  The rationale is that as T is less than or equal to -2, the likelihood category must be 1 or 2. Therefore, the consequence category must be no greater than 2 to limit the uncontrolled risk index to 4 at most. In this case, the uncertainty in determining a low failure likelihood requires compensatory measures in the form of increased assurances (high-level criteria) that the IROFS is indeed kept at a low failure likelihood.

A.11 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.

Accession #: ML013370311