APPENDIX A

EXAMPLE PROCEDURE FOR ACCIDENT SEQUENCE RISK EVALUATION

[Comment: the first page of the appendix provides background information that repeats what has already been presented in Chapter 3 (e.g. §3.1, §3.3.1, etc.). Such material, while informative and consistent with the rule and SRP guidance, need not be repeated here, particularly as the appendix is not a stand-alone document. For the sake of simplicity and clarity, we recommend replacing the background information by the following brief introduction. We also recommend that the introduction clarify that the appendix does not constitute a 'format and content' guide for either the ISA or ISA Summary.]

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 which accident sequences have consequences that could exceed the performance requirements of 10 CFR 70.61 and, therefore, require designation of 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.

This appendix is not a "format and content guide" for either the ISA or the ISA Summary. It simply presents one method to ensure the consistent and thorough analysis and categorization of credible accident sequences for facility processes.

~~10 CFR 70.61 defines two consequence categories, high and intermediate, by specifying quantitative radiological dose levels and qualitative chemical health-effects levels. Section 70.61 further requires that intermediate-consequence events be unlikely, and high-consequence events be highly unlikely. These requirements are referred to as "performance requirements." 10 CFR 70.62 requires that the applicant perform an Integrated Safety Analysis (ISA) to identify all potential accident sequences, to assess their consequences, and to evaluate compliance with these consequence-likelihood performance requirements. The applicant is to convert the qualitative chemical levels into quantitative standards.~~

~~This appendix describes one method of evaluating compliance with the consequence-likelihood performance requirements of 10 CFR 70.61. The method is intended to permit quantitative information to be considered, if available. For consistency, the staff's approach could also include assigning quantitative values to any qualitative likelihood assessments made by the licensees 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 controls involved.~~

~~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 in Tables A-8 and A-9, are intended to be examples, not universal criteria. It~~

is preferable that each applicant develop such criteria, based on the particular types of controls and management measure programs in the facility evaluated. Such criteria should be modified and improved as insights are gained during performance of the ISA.

[Comment: the following sentence is identical to the first sentence in paragraph 2. Delete as redundant.]The procedure described in this appendix is one method by which the applicant may use the ISA results to demonstrate that the requirements of 10 CFR 70.61 have been met. If the licensee evaluates accidents using a different method, the method should produce similar results in terms of how accidents are categorized. This method should be regarded as a screening method, not as a definitive method of proving the adequacy or inadequacy of the controls 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 controls used to limit accident sequences. This will permit identification of accident sequences with defects in the combination of controls used. Such controls can then be further evaluated or improved to establish adequacy. The procedure also ensures the consistent evaluation of similar controls by different ISA teams. Sequences or controls 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 controls 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 controls, such that the performance requirements of 10 CFR 70.61 are met. These criteria require that controls 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 DEVELOPMENTDETERMINING COMPLIANCE WITH GRADED PROTECTION REQUIREMENTS

Consequences:

~~Section 70.61 of 10 CFR Part 70 describes requirements for a system of protection sufficient to limit the risk of identified accidents by making accidents of higher potential consequences have a proportionately lower likelihood of occurrence. The regulation~~ 10 CFR 70.61 specifies two categories for accident sequence~~of~~ consequences: ~~into which an accident may fall. The first category is referred to in 10 CFR 70.61 as~~ "high consequences~~,~~" and ~~the second as~~ "intermediate consequences." Implicitly there is a third category for ~~namely, those~~ accidents that produce consequences less than "intermediate." These will be referred to as "low-consequence" accident sequences. [Comment: the following sentence is a little too restrictive. The PHA should identify all accident sequences regardless of their consequences. Following categorization of the accidents by consequence, the subsequent ISA analysis just focuses on accidents in the two most safety-significant categories. Recommend some clarification in the language.] The ~~Since the~~ primary purpose of Process Hazard Analysis is to identify all uncontrolled and unmitigated accident sequences. ~~having consequences that exceed the levels in 10 CFR 70.61, it will, in some cases, identify uncontrolled and unmitigated accidents, which produce radioactive or chemical exposures that do not exceed the threshold values for intermediate consequences. For this reason, in the method described here, the table listing accidents is intended to include such low-consequence accidents to show that they have been considered.~~ These accident sequences can then be categorized into one of these three consequence categories (high, intermediate, low) based on their forecast radiological, chemical and environmental impacts. Although the subsequent ISA analysis focuses only 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.~~If they are not listed, some other demonstration of the completeness of the accident-identification task should be provided in the ISA Summary.~~ Table A-1 presents the radiological and chemical consequence severity limits of 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**
Consequence Category 3: High	D>1 Sv (100 rem)	D>0.25 Sv (25 rem) 30 mg sol U intake	
Consequence Category 2: Intermediate	0.25 Sv(25 rem)<D≤ 1 Sv (100 rem)	0.05 Sv(5 rem)<D≤ 0.25 Sv (25 rem)	Radioactive release >5000 x Table 2 App B 10 CFR Part 20
Consequence Category 1: Low	Accidents of lesser radiological and chemical exposures to workers than those above, in this column	Accidents of lesser radiological and chemical exposures to the public than those above in this column	Radioactive releases producing effects less than those specified above in this column

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 accident can have a likelihood of occurrence less than "unlikely", or simply "not unlikely." The likelihood of occurrence limits of 70.61 are portrayed in Table A-2 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"[1]

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 or 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 whose consequences and likelihood yield an unacceptable risk index and for which IROFS will have to be applied.

Table A-3: Risk Matrix with Risk Index Values

	Likelihood of Occurrence		
Severity of Consequences	Likelihood Category 1 Highly Unlikely (1)	Likelihood Category 2 Unlikely (2)	Likelihood Category 3 Not Unlikely (3)
Consequence Cat. 3 High (3)	Acceptable Risk (10 CFR 70.65) 3	Unacceptable Risk 6	Unacceptable Risk 9
Consequence Cat. 2 Intermediate (2)	Acceptable Risk 2	Acceptable Risk (10 CFR 70.65) 4	Unacceptable Risk 6
Consequence Cat. 1 Low (1)	Acceptable Risk 1	Acceptable Risk 2	Acceptable Risk 3

[1] Implicitly this is a third category into which an accident could fall, i.e., it could fail to be "unlikely". Although this category includes unintended events that might actually be expected to happen, others might be less frequent. For this reason, the term "likely" was not used for these events.

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 either 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 ~~conforms to~~ the ~~safety~~ 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 qualitative Risk Index Method the likelihood index for the uncontrolled and unmitigated accident sequence is adjusted by subtracting a score appropriate 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, then 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 section 3.4.3.2, subsections 5 and 7.

Table A-4: Qualitative Categorization of IROFS

Numerical 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 an active engineered IROFS in addition to trained operator 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)**

~~The limits defining the three accident-consequence categories are given below. Note that the categories are numbered in ascending order of the magnitude of their consequences. The~~

usefulness of this numbering will be evident later. The Acute Exposure Guideline Level (AEGL) and Emergency Response Planning Guideline (ERPG) refer to chemical-exposure levels from accidents sufficient to produce certain effects. AEGL-3 and ERPG-3 levels are life-threatening. Part 70 does not specify the use of AEGL or ERPG levels. 10 CFR 70.61(b) and (c) require applicants to propose quantitative exposure levels that they would use in the two primary consequence categories below. AEGL and ERPG levels are acceptable for those substances for which the levels have been determined by the appropriate agencies, and are described here.

Consequence Category 3- High Consequences: An accident 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)[2] total effective dose equivalent (TEDE); or (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; or (c) chemical exposures that could lead to irreversible or other serious long-lasting health effects (exceeding AEGL-2 or ERPG-2).

Consequence Category 2- Intermediate Consequences: An accident resulting in any consequence specified in 10 CFR 70.61(c). These include, (1) acute exposures of workers to: (a) a radiation doses between 0.25 Sievert (25 rem) and 1 Sievert (100 rem) TEDE; or (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-1 or ERPG-1); or (3) prompt release of radiation 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: Any accident with potential adverse radiological or chemical consequences, but at exposures less than Categories 3 and 2, above.

This system of consequence categories is shown in Table A-1. In this table, "D" signifies the TEDE from an acute accidental radiation exposure.

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

	Workers	**Offsite Public**	**Environment**
Consequence Category 3: High	D>1 Sv (100 rem) >AEGL-3, ERPG-3	D>.25 Sv (25 rem) 30 mg sol U intake >AEGL-2, ERPG-2	
Consequence	.25 Sv(25 rem)<D≤ 1	.05 Sv(5 rem)<D≤ .25	Radioactive release >5000 x

[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.

	Workers	Offsite Public	Environment
Category 2: Intermediate	Sv (100 rem) >AEGL-2, ERPG-2 but <AEGL-3, ERPG-3	Sv (25 rem) >AEGL-1, ERPG-1 but <AEGL-2, ERPG-2	Table 2 App B 10 CFR Part 20
Consequence Category 1: Low	Accidents of lesser radiological and chemical exposures to workers than those above, in this column	Accidents of lesser radiological and chemical exposures to the public than those above in this column	Radioactive releases producing effects less than those specified above in this column

Corresponding to the two consequence categories of 10 CFR 70.61 (Categories 2 and 3 in Table A-1), engineered and administrative controls and management measures must be provided sufficient to ensure that the likelihoods of these adverse events are correspondingly low. The categories of likelihood are shown in Table A-2.

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"[3]

The ISA is meant to initially identify credible uncontrolled and unmitigated accidents that exceed Consequence Category 2 and 3 levels. After this determination, the ISA is intended to identify items relied upon for safety (IROFS) that would ensure that the probability of occurrences of accidents that exceed Consequence Category 2 and 3 levels are "unlikely" and "highly unlikely," respectively. As such, compliance with the performance requirements of 10 CFR 70.61 can be demonstrated by implementing a graded system of protection that adequately reduces the uncontrolled and unmitigated consequences and likelihoods of the accidents.

A major purpose of the ISA is to show compliance with the above system of graded protection. This can be done by using the required tabular summary of identified accident sequences. One acceptable way of doing so is for the applicant to assign two category numbers to each of these accident sequences with the system of protection in place, one based on its consequences and

[3] Implicitly this is a third category into which an accident could fall, i.e., it could fail to be "unlikely". Although this category includes unintended events that might actually be expected to happen, others might be less frequent. For this reason, the term "likely" was not used for these events.

one for likelihood. The product of these two category numbers is then used as a risk index. Listing this calculated risk index in the tabular summary provides a simple method for showing that the graded protection requirements have been met for each accident sequence. A risk index value less than or equal to "4" means the sequence is acceptably protected and/or mitigated. If the applicant provides this risk index in one column of the tabular summary, the reviewer can quickly scan this column to confirm that each accident conforms to the safety performance requirements of 10 CFR 70.61. This system is equivalent to assigning each protected and/or mitigated accident to a cell in a 3 by 3 matrix. This conceptual matrix is shown in Table A-3 below. The values in the matrix cells are the risk index numbers.

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 Cat. 3 High (3)	Acceptable Risk (10 CFR 70.65) 3	Unacceptable Risk 6	Unacceptable Risk 9
Consequence Cat. 2 Intermediate (2)	Acceptable Risk 2	Acceptable Risk (10 CFR 70.65) 4	Unacceptable Risk 6
Consequence Cat. 1 Low (1)	Acceptable Risk 1	Acceptable Risk 2	Acceptable Risk 3

To demonstrate compliance with the performance requirements of 10 CFR 70.61 the system described above, the applicant needs to assign a consequence categoryies to each identified accident sequence. to determine which likelihood requirement applies. Then the likelihood of occurrence of those accident sequences identified as high- or intermediate--consequences events must then be assigned to one of the three a likelihood categoriesy. To be acceptable, the controlled and/or mitigated accident consequences and likelihoods must have valid bases, and the applicant must demonstrate 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 to be a "high consequence event" or an "intermediate consequence event," or neither, The assignment of consequence categories is based on the estimated consequences of prototype accidents. Although accident consequences of accidents can be determined by actual calculations, calculations need not be it is not necessary that such a calculation 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 its processing. 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: An accident 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)[4] total effective dose equivalent (TEDE); or (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; or (c) chemical exposures that could lead to irreversible or other serious long-lasting health effects (exceeding AEGL-2 or ERPG-2).

Consequence Category 2- Intermediate Consequences: An accident resulting in any consequence specified in 10 CFR 70.61(c). These include, (1) acute exposures of workers to: (a) a radiation doses between 0.25 Sievert (25 rem) and 1 Sievert (100 rem) TEDE; or (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-1 or ERPG-1); or (3) prompt release of radiation 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: Any accident with potential adverse radiological or chemical consequences, but at exposures less than Categories 3 and 2, above.

This system of consequence categories is shown in Table A-5. In this table, "D" signifies the TEDE from an acute accidental radiation exposure.

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

	Workers	**Offsite Public**	**Environment**
Consequence Category 3: High	D>1 Sv (100 rem) >AEGL-3, ERPG-3	D>.25 Sv (25 rem) 30 mg sol U intake >AEGL-2, ERPG-2	
Consequence Category 2: Intermediate	.25 Sv(25 rem)<D≤ 1 Sv (100 rem) >AEGL-2, ERPG-2 but <AEGL-3, ERPG-3	.05 Sv(5 rem)<D≤ .25 Sv (25 rem) >AEGL-1, ERPG-1 but <AEGL-2, ERPG-2	Radioactive release >5000 x Table 2 App B 10 CFR Part 20

[4] 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.

	Workers	Offsite Public	Environment
Consequence Category 1: Low	Accidents of lesser radiological and chemical exposures to workers than those above, in this column	Accidents of lesser radiological and chemical exposures to the public than those above in this column	Radioactive releases producing effects less than those specified above in this column

Regardless of the chemical exposure standards selected, tThe 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 safety controls at the facility or other methods that have objective validity. Because sequences leading to accidents often involve multiple failures, a combination of failure frequency and probability values determines the likelihood of the whole sequence will depend on . These values include the frequencies of initiating events and failure likelihoods of engineered and administrative IROFS. controls. An acceptable method is described below, by which the applicant can make an estimate of an approximate likelihood category for an accident sequence by considering all the events involved. The method of likelihood assignment used in this Appendix relies on the expert engineering judgement of the analyst and includes assessment This method makes use of the number, type, independence, and observed failure history of designated IROFS. controls, as evaluated by an applicant using expert engineering judgment. Thus, a reasonably accurate evaluation of the appropriate estimated likelihood of accidents using such a qualitative system depends on the informed judgement of the analyst. Engineered and administrative IROFS, controls, even those of the same types, have a wide range of reliability. The ultimate criterion for acceptability is that the frequencies of initiating events and the likelihoods of failure of controls involved are sufficiently low so that the entire accident sequence is "highly unlikely" or "unlikely," as required by 10 CFR 70.61. The virtue of the method is that it By requiring requires explicit consideration of most of the underlying events and factors that significantly affect the likelihood of the accident and . Another virtue is that the use of explicit criteria to assign likelihood, greater consistency in assigning likelihood to accident sequences yields more consistent results across different systems within a plant and among different applicants should be possible.

[Comment: consistent with the significant revisions made to §3.4.3.2 Item (9) under 'Quantitative Guidelines' the detailed explanation as to how the NRC arrives at the 10^{-5} and 10^{-4} frequency standards is no longer needed in the appendix. We recommend the following simplification. For the sake of consistency, we also recommend using the same Chapter 3 terminology in the appendix: "*per-event per-year*" rather than "*per accident per year*".]

Quantitative measures of likelihood are based on the NRC's determinations reported in Item (9) of §3.4.3.2 of SRP Chapter 3: "highly unlikely" means a frequency of less than one accident in the industry per year, or 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. ~~Underlying any evaluation of an accident sequence as "unlikely" or "highly unlikely" is an implied assessment of its "likelihood" or frequency of occurrence. The method described below will indicate which likelihood category may be appropriate for an event. To maintain internal consistency in evaluating different control systems and accidents, it was necessary to derive this method based on the underlying frequencies of events. The numerical guidelines contained in Table A-4, below, were thus used to obtain consistency and to be consistent with staff safety goals.~~

Table A-~~4~~6: Event Likelihood and Numerical Scores

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

In assessing the adequacy of engineered and administrative IROFS~~controls~~, individual accident frequencies greater than 10^{-5} per year may not be evaluated as "highly unlikely." ~~The safety goal underlying this frequency limit is that no inadvertent nuclear criticalities occur in the industry. This goal is here interpreted as limiting the frequency of such accidents in the industry to not more than once in 100 years (0.01 per year). This is then converted to a "per-accident" frequency by dividing by an estimated number of potential accidents for the whole industry. An estimate of 1000 accidents has been used. Thus 0.01 per year/1000 accidents =10^{-5} per year per accident.~~

~~The value of 10^{-5} per year per accident is such that a plant with 100 potential Consequence Category 3 accidents would have a frequency of: 100 accidents times 10^{-5} per year per accident = 10^{-3} per year. These Category 3 accidents generally result in fatalities. The average statistic for all manufacturing industries is that a plant with 250 manufacturing workers would expect 10^{-2} on-the-job deaths per year (see References, "Statistical Abstract of the U.S.").~~

Similarly, accident sequences having frequencies more than 10^{-4} per year per accident are not considered "unlikely." ~~Again this value should not be taken as a definitive criterion for acceptability. It is a guideline value to assure consistency. It will need to be adjusted based on the numbers and severity of accidents. This frequency is chosen based on a goal that the frequency of events comparable to 0.25 Sv (25 rem) worker exposures not increase above its current 5 year average of 0.4 per year. Since this goal is for all Nuclear Regulatory Commission (NRC) licensees, only a fraction can be allocated to the part of the industry addressed by this SRP. Again a "per-accident" limit must be derived that depends on the total number of accidents in the industry. For an allocation of one-tenth and an estimate of 1000 intermediate-consequence accidents in the industry, a value of 4x10^{-5} per accident per year was obtained. However, since this value is a goal, and the actual number of accidents has not yet been determined, a value of less than 10^{-4} is considered a reasonable guideline at the inception of structured risk analysis by the fuel cycle industry.~~

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. ~~The reason d~~Double contingency is needed as ~~is the fact that~~ there are ~~is~~ usually insufficient firm data as to the reliability of the IROFS ~~control~~ equipment and administrative ~~control~~ 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, ~~it is prudent to have~~ at least two independent IROFS should be used ~~controls~~. Inadequate IROFS ~~controls~~ can then be determined by observing their failures, without also suffering the consequences of criticalities. Even with double contingency, ~~it is essential that~~ each IROFS should be sufficiently unlikely to fail- for~~. This is so that~~ if one of the two items that establish double contingency is actually ineffective, criticality will still be unlikely.

~~A.4 QUALITATIVE CATEGORIZATION OF IROFS~~

~~A qualitative categorization of IROFS is provided in Table A-5 below. As in the quantitative approach, the likelihood indexes for an uncontrolled and unmitigated accident may be adjusted by subtracting the appropriate IROFS score.~~

~~Reviewers should note that the coarse qualitative criteria for evaluation of controls (IROFS) in Tables A-5, A-8, and A-9 are given as illustrations only. IROFS meeting the criteria for a particular score in these tables 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, then a more careful evaluation should be done. Such evaluations should consider the management measures applied to all the reliability and availability qualities of the set of IROFS protecting against the accident, as explained in the likelihood acceptance criteria of this chapter in section 3.4.3.2, subsections 5 and 7.~~

~~Table A-5: Qualitative Categorization of IROFS~~

~~Numerical Value~~	~~Description of IROFS~~
~~1~~	~~Protection by a single, trained operator with adequate response time~~ **~~(Administrative Control)~~**
~~2~~	~~Protection by a single active engineered control, functionally tested on a regular basis~~ **~~(Active Engineered Control)~~**
~~3~~	~~Protection by a single passive-engineered control, Functionally tested on a regular basis, or an active engineered control in addition to trained operator back-up.~~ **~~(Passive Engineered Control or Combined Engineered and Administrative Controls)~~**
~~4~~	~~Protection by two independent and redundant engineered controls, as appropriate, functionally tested on a regular basis~~ **~~(Combination of Two Active or Passive Engineered Controls)~~**

A.4~~5~~ 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 its consequences to an acceptable level, IROFS can reduce the overall resulting risk. The designation of IROFS should generally be made to reduce the likelihood (i.e., prevention of 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 whose ~~where the~~ resulting unmitigated or uncontrolled risks are unacceptable, key safety controls (administrative and/or engineered controls) may be designated as IROFS to reduce the likelihood of occurrence and/or mitigate the consequence severity.

A.5~~6~~ 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-~~6~~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-~~6~~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. A summary of the risk index calculation will be given below.

Accident sequences result from initiating events, followed by failure of one or more ~~controls~~IROFS. Thus there are columns, in Table A-7~~6~~, for the initiating event and for IROFS~~controls~~. IROFS~~Controls~~ may be mitigative or preventive. Mitigative IROFS~~controls~~ 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 ~~controls~~ fails and mitigation also fails. Mitigated consequences result when the preventive IROFS~~controls~~ fail, but mitigative measures succeed. These are abbreviated in the table as "unmit." and "mitig.," respectively. Index numbers are assigned to initiating events, IROFS~~control~~ failure events, and mitigation failure events, based on the reliability characteristics of these items.

With redundant IROFS~~controls~~ and in certain other cases~~,~~ there are sequences in which ~~where~~ an initiating event ~~occurs that~~ places the system in a vulnerable state. While the system is in this vulnerable state, an IROFS ~~control~~ 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) ~~control~~ IROFS failure. For this reason, ~~it is necessary to consider~~ the duration of the vulnerable state should be considered~~,~~ and ~~to assign it~~ 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 s~~S~~equences 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~~7~~.

The values of index numbers in accident sequences are assigned considering the criteria in Tables A-9~~8~~ through A-11~~10~~. Each table applies to a different type of event. Table A-9~~8~~ applies to events that have frequencies of occurrence, such as initiating events and certain ~~control~~ IROFS failures. When failure probabilities are required for an event, Table A-10~~9~~ provides the index values. Table A-11~~10~~ provides index numbers for durations of failure. These are used in certain accident sequences where two IROFS~~controls~~ 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." The first failure may 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~~controls~~ 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 ~~control~~ 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 second IROFS~~control~~ may differ from that of the first. 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.

As shown in Table A-11~~10~~, the duration of failure is accounted for in establishing the overall likelihood that an accident sequence would 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 applicant's chosen duration of failure index, and the defined risks (reported in the ISA Summary) associated with the consequences are acceptable pursuant to 10 CFR 70.61, then when such failures occur, it does not imply a violation of the approved license.

For all these index numbers, the more negative the number is, the less likely is 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~~6~~, 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, to be acceptable, should be based on the existence of intentional monitoring of the process. The duration of failure for an unmonitored process should be conservatively estimated.

Table A-7~~6~~ provides two risk indices for each accident sequence, to permit evaluation of the risk significance of the IROFS ~~controls~~ involved. To measure whether an IROFS ~~control~~ has high-risk significance, the table provides an "uncontrolled risk index," determined by modeling the sequence with all IROFS ~~controls~~ 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 ~~control~~ failures. When an accident sequence has an uncontrolled risk index exceeding 4, but a controlled index of less than 4, then the IROFS ~~controls~~ involved have a high-risk significance in that they are relied on to achieve acceptable safety performance. Thus, use of these indices permits evaluation of the possible benefit of improving IROFS ~~controls~~, and also whether a relaxation may be acceptable.

Table A-1211 provides a more detailed description of the accident sequences used in the example of Table A-76. The reviewer needs the information in Table A-1211 to understand the nature of the accident sequences listed in Table A-76. Table A-76 lacks sufficient room to explain any but the simplest failure events.

Table A-1312 is used to explain the controls IROFS and external initiating events that appear in the accident sequences in Table A-76. The reviewer needs the information in Table A-1312 to understand why the initiating events and IROFScontrols listed in Table A-67 have the low likelihood indices assigned. Thus, Table A-1312 needs to address such information as: 1) the margins to safety limits; 2) the redundancy of an controlIROFS; and 3) the measures taken to assure adequate reliability of an IROFS control. Table A-1312 must also justify why those 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 IROFScontrols for criticality, chemical, fire, radiological, and environmental accidents.

Table A-7~~6~~: 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 Sequence	Initiating Event (a)	Preventive IROFS~~Control~~ 1 (b)	Preventive IROFS~~Control~~ 2 (c)	Mitigation IROFS~~Control~~ (d)	Likelihood* Index T (e) uncontrolled controlled	Likelihood Category (f)	Conse-Quence Evaluation Reference	Conse-quence Category (g)	Risk Indices (h=f x g) uncontrolled controlled	Comments & Recommendations
PPB2-1A (Criticality from blender leak of UO_2)	See ~~Control~~ IROFS1 (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 1	Rad 35	3 (Crit: 3, rad: 0)	9 3	Criticality, consequences = 3 Control 2 fails while Control 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, OR	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 ~~control~~ 1 & mitigation fail. T= -1-3 = -4 Mitig.: IROFS~~Control~~ 1 fails, mitig. IROFS~~control~~ does not fail. T = -1
PPB2-1C	See IROFS ~~Control~~ 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 = -1	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~~control~~ 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~~controls~~, hence the frequency is assigned under that ~~control~~IROFS.

Table A-~~7~~8: Determination of Likelihood Category

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

Table A-~~8~~9: Failure Frequency Index Numbers

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

* Indices less than (more negative than) “-1" should not be assigned to IROFScontrols unless the configuration management, auditing, and other management measures are of high quality, because, without these measures, the IROFScontrols may be changed or not maintained.

** The index value assigned to an IROFS control 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-~~9~~10-: Failure Probability Index Numbers

Probability Index Number	Probability of Failure on Demand	Based on Type of ~~Control~~IROFS	Comments
-6 *	10^{-6}		If initiating event, no ~~controls~~ IROFS needed
-4 or -5*	10^{-4} - 10^{-5}	Exceptionally robust passive engineered control (PEC), or an inherently safe process, or 2 redundant IROFS~~controls~~ better than simple admin IROFS~~controls~~ (AEC, PEC, or enhanced admin)	Rarely can be justified by evidence, since few systems are found in such large numbers . Further, most types of single IROFS~~control~~ have been observed to fail.
-3 or -4*	10^{-3} - 10^{-4}	A single passive engineered ctrl. (PEC) or an active engineered control (AEC) with high availability	
-2 or -3 *	10^{-2} - 10^{-3}	A single active engineered IROFS~~control~~, or an enhanced admin IROFS~~control~~, or an admin IROFS~~control~~ for routine planned operations	
-1 or -2	10^{-1} - 10^{-2}	An admin IROFS~~control~~ that must be performed in response to a rare unplanned demand	

* Indices less than (more negative than) "-1" should not be assigned to ~~controls~~ IROFS unless the configuration management, auditing, and other management measures are of high quality, because, without these measures, the ~~controls~~ IROFS may be changed or not maintained.

Table A-11~~10~~: Failure Duration Index Numbers

Duration Index Number	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}	

DRAFT

Table A-~~11~~12: Accident Sequence Descriptions

Process: Uranium dioxide (UO_2) Powder Preparation (PP) Unit Process: 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 UO_2 can be removed, moderator sufficient to cause criticality is introduced. Duration of critical mass UO_2 on floor estimated to be one 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 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, 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. Release of UO_2 from process equipment occurs. Offsite dose estimated to exceed 1 mSv (100 mrem).

Table A-1312: Descriptive List of Items Relied on for Safety

Process: Uranium dioxide (UO_2) Powder Preparation (PP) Unit Process: Additive Blending
Node: Blender Hopper Node (PPB2)

IROFS Safety Control Identifier	Safety Parameter and Limits	IROFS Safety Controls Description	Max Value of Other Parameters
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%
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%

Note: In addition to engineered controlsIROFS, this table should include descriptions of external initiating events whose 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.67 ACCIDENT SUMMARY AND RISK INDEX ASSIGNMENT FOR TABLE A-76

The definitions for the contents of each column in the accident summary tabulation, Table **A-**7**6**, are provided below.

Accident Sequence
[Comment: listings of the accident sequences in Table A-7 are not expected in the ISA Summary. 10 CFR 70.65(b)(3) only requires a listing of the general types of accident sequences. There appears to be some confusion in these Sections A-7 through A-12 as to the amount of detailed information that should be provided in the ISA and ISA Summary. This is a very important distinction.]

This column is provided to lists the accident sequences identified by the applicant in the ISA Summary. Accident sequences should be presented for It is important to the proper documentation of the ISA that the applicant subdivides the plant into a set of uniquely identified facility processesunits, referred to here as “nodes.” The applicant should give symbols, names, or numbers to these nodes that permit them to be uniquely identified. For example, the “Blender Hopper” node described In Table A-7**6** has the unique identifying symbol PPB2. Additional identifier characters have been added to form the identifier, PPB2-1, to identify the first accident sequence identified in that node. Because the applicant should list all the plant IROFS controls of significance used elsewhere in the ISA, tabulations of the unique node (and accident) identifier can be used to find the accidents that these controls IROFS have been designated shown to prevent. By reviewing this table, the reviewer can then evaluate: (1) the adequacy of the IROFS ~~controls~~ for preventing accidents; and (2) the bases for making the consequence and likelihood assignments in the table.

Initiating Event or ~~Control~~ IROFS Failure (Column (a))
This column ~~is provided to~~ lists initiating events or IROFS ~~control~~ failures, typically identified in the Process Hazard Analysis phase of the ISA, 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) plant events external to the node being analyzed (e.g., fires, explosions, failures of other equipment, flooding from plant-water sources); (3) deviations from normal operations of the process in the node (i.e., credible abnormal events); and (4) failures of IROFS ~~controls~~ of the node. The tabulated initiating events should only consist of those that involve an actual or threatened failure of ~~controls~~IROFS, or that cause a demand requiring ~~controls~~ 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 using the symbol "frqi." Table A-9~~8~~ provides criteria for assigning a value to frqi. Usually, insufficient room is present in a tabular presentation like Table A-7~~6~~ to describe accurately the events indicated. Consequently, the applicant should provide supplementary narrative information to adequately describe each general type of accident sequence of Table A-7~~6~~. Cross-referencing between this information and the table should be adequate (eg., the unique symbolic accident sequence identifiers can be used). Table A-12~~11~~ is an example of a list of supplementary accident sequence descriptions corresponding to Table A-6.

Preventive IROFS ~~Control~~ 1 (Column (b))
This column ~~is provided to~~ lists an IROFS ~~control~~ designated to prevent consequences exceeding 10 CFR 70.61 levels. If separate IROFS ~~controls~~ are used to prevent different consequences, separate rows in the table should be defined corresponding to each type of consequence. Table A-7~~6~~ contains an example of a set of related sequences so separated. Accident s~~S~~equences where two IROFS ~~controls~~ must simultaneously be in a failed state require assignment of three index numbers: the failure frequency of the first IROFS~~control~~, frq1, the duration of this failure, dur1, and the failure frequency of the second IROFS~~control~~, frq2. For such accident sequences, the initiating event is failure of the first IROFS~~control~~. In these cases, frq1 is assigned using Table A-9~~8~~. The failure duration of the first IROFS~~control~~ is assigned using Table A-10. Other accident sequences may be more easily described as a failure of the IROFS~~safety controls~~ on demand after the occurrence of an initiating event. In these cases, the failure probability index number, prf1, is assigned using Table A-10~~9~~. ~~The symbol "b" is used in the column heading for the indices associated with this control.~~

Preventive IROFS~~Control~~ 2 (Column (c))
This column is provided in case a second preventive IROFS ~~control~~ is designated ~~exists~~. The failure frequency or failure probability on demand is assigned as for Preventive ~~Control~~ IROFS 1. ~~The symbol "c" is used in the column heading for the indices associated with this control.~~

Mitigation IROFS~~Control~~ (Column (d))
This column is provided in case IROFS~~controls~~ 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 ~~control~~ that eliminates all adverse consequences should be considered preventive. ~~The symbol "d" is used in the column heading for the indices associated with this control.~~

Likelihood Index (Column (e)) and Likelihood Category (Column (f))

This column is provided to 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. These events normally consist of the initiating event, and failure of one or more IROFScontrols, 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-87. The symbol "e" is used for this category number in the column heading.

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, various chemicals, 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) that may occur. Based on this estimate, accidents can be assigned to the categories defined in 10 CFR 70.61. The symbol "f" is used for this category number in the column heading. Accident sSequences having IROFScontrols 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-76, 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
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 "g = e x f." Sequences with values of "g" 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 IROFScontrols. For example, in the first three cases in Table A-76, the initiating event is failure of Preventive Control IROFS 1. In these cases, the failure frequency of Preventive IROFSControl 1 is used to determine the likelihood category when calculating the unmitigated risk index.

Comments and Recommendations
This column is needed to record ISA team recommendations, especially when the existing system of IROFScontrols is evaluated as being deficient. This may happen because a newly identified accident sequence is not addressed by existing IROFScontrols, or because a deficiency has been found in the existing IROFScontrols.

A.8 DETERMINATION OF LIKELIHOOD CATEGORY IN TABLE A-87

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.

A.9 DETERMINATION OF FAILURE FREQUENCY INDEX NUMBERS IN TABLE A-98

Table A-98 is used to assign frequency index numbers to plant initiating events and IROFScontrol system failures as found in the columns of Table A-76. The term "failure" must be understood to mean not merely failure of the IROFScontrol device or procedure, but also as a violation of the process safety limit by the process. In the example in Table A-76, 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 IROFScontrol failures do not cause safety limits to be exceeded.

Table A-98 provides two columns with two sets of criteria for assigning an index value, one based on type of IROFScontrol, the other directly on observed failure frequencies. The types of controls are administrative, active engineered, passive engineered, etc. Since IROFScontrols 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 as to whether the IROFS control 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 Control,” references to redundancy allow for controls 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 plant or in a comparable process elsewhere. Justification for specific assignments may be noted in the Comments column of Table A-76.

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

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

A.10 DETERMINATION OF FAILURE PROBABILITY INDEX NUMBERS IN TABLE A-109

Occasionally, information concerning the reliability of an IROFS safety control may be available as a probability on demand. That is, a history may exist of tests or incidents where the system in question is demanded to function. To quantify such accident sequences it is necessary then to

~~know~~ the demand frequency, the initiating event, and the demand failure probability of the IROFS~~safety control~~ must be known. This table provides an assignment of index numbers for such IROFS controls in a way that is consistent with Table A-9~~8~~. 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 mission.

A.11 DETERMINING MANAGEMENT MEASURES FOR IROFS ~~SAFETY CONTROLS~~

Table A-1~~2~~3 is an acceptable way of listing those IROFS in all the general types of accident sequences leading to consequences exceeding those identified in 10 CFR 70.61. The items listed should include all IROFS~~safety controls~~ and all external events whose low likelihood is relied upon to meet the performance requirements of 10 CFR 70.61. Staff reviews this list to determine whether measures have been applied to each IROFS~~safety control~~, adequate to assure its continual availability and reliability, in conformance to 10 CFR 70.62(d). The types of management measures include 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 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 ~~controls~~ IROFS on a process, this minimal set of measures must include an adequate degree of: a) configuration management; b) regular auditing for the continued effectiveness of the ~~control~~IROFS; c) adequate labeling, training, or written procedures to ensure that the operating staff is aware of the safety function; d) surveillance and corrective maintenance; and e) preventive maintenance, if applicable.

If lesser or graded management measures are applied to some IROFS~~controls~~, Tables A-7~~6~~ and A-13~~12,~~ and the narratives preceding them~~, to be acceptable,~~ must identify to which IROFS~~controls~~ these lesser measures are applied. In addition, information indicating that acceptable reliability can be achieved with these lesser measures must be presented. ~~It is not necessary that~~ The specifics of how each management measure ~~these measures~~, such as the surveillance interval, type of maintenance, or type of testing, is~~be described, as~~ applied to each IROFS need not be provided~~control~~, for the NRC recognizes that ~~. It is recognized that~~ such specific measures must be applied differently to each ~~control~~IROFS~~, to whatever degree is necessary~~ to achieve adequate reliability. ~~It is t~~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 describes 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 ~~6 of Appendix A to this Chapter;~~ and (2) the accident likelihood index, “T,” also described in Table A-7~~6~~. [Comment: the following statement does not seem consistent with the rule or Chapter 3 guidance. Compliance with the provisions of 70.64 should only be expected for new facilities or for new processes at existing facilities that require a license amendment. Revise]. In summary, items relied on to prevent or mitigate accidents that would have unmitigated consequences in the two highest categories identified in 10 CFR 70.61 should satisfy the following requirements:~~Baseline Design Requirements of 10 CFR 70.64 that apply.~~

1. For those accident sequences that are reduced in risk from initially high risk (an "uncontrolled" risk index of 6 or 9, from Section A.1 of Appendix A) to an acceptable risk ("controlled" risk index of less than or equal to 4):

[Comment: the following criterion is puzzling. The topic of this Section A.11 is management measures, and so we don't see how BDC should be relevant. Furthermore, if we are addressing an existing facility, 10 CFR 70 would exclude consideration of the BDC. Some clarification is needed.]~~IROFS must have satisfied all applicable Baseline Design Requirements of 10 CFR 70.64.~~

2. 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 2.B below), yet be of low consequence such that the risk is acceptable without ~~controls~~IROFS. However, if the accident consequence of interest is a nuclear criticality, 10 CFR 70.61(d) requires that this consequence be limited in likelihood to "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~~, typically a control,~~ in addition to the initiating event. ~~This control must have satisfied all applicable Baseline Design Requirements of 10 CFR 70.64.~~ With this exception for criticality sequences, the following three cases apply:

2A. If the initiating event is not an IROFS ~~control~~ failure, then 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 frequency must be adequately justified in the application.

2B. If the initiating event is an IROFS ~~control~~ failure, and if the likelihood of that failure is taken to be more than a few times per plant lifetime (T is greater than -2), then assurances for that item relied on may be less ~~than the Baseline Design Requirements of 10 CFR 70.64, as defined by the applicant and approved by NRC.~~ Any subsequent IROFS ~~items~~ in the accident sequence will be unregulated.

[Rationale: Since T is greater than -2, the likelihood category is 3. Therefore the consequence category is no greater than 1, to limit the uncontrolled risk index to, at most, 4. Since the consequence category is low, the assurance level can be reduced]

2C. If the initiating event is an IROFS~~control~~ failure, and if the likelihood of that failure is taken to be less than a few times per plant lifetime (T is less than or equal to -2), then assurance for this IROFS~~control~~ must satisfy the full Baseline Design Requirements. No regulation of subsequent IROFS ~~controls~~ in the sequence is necessary.

[Rationale: Since 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 at most 4. 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 ~~control~~ is indeed kept at a low failure likelihood]

A.12 RISK-INFORMED REVIEW OF IROFS

[Comment: this paragraph appears redundant. Its issues have been addressed in Chapter 3. Recommend deletion.]~~NRC staff will review the IROFS failures and external events listed in Table A-12 in a risk-informed manner. Accident sequences having potential for higher risk will be subject to a more detailed staff review, to assure their adequacy.~~

[Comment: the following sentence is correct when applied to the ISA, but the statement at the beginning of Section A-8 that the Appendix tables contain the information appropriate to the ISA Summary, makes this sentence erroneous.] The final-results column of Table A-7~~6~~ 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~~safety controls~~. If the uncontrolled risk index is a 6 or 9, while the controlled index is an acceptable value (less than 5), the set of IROFS~~safety controls~~ involved are significant in achieving acceptable risk. That is, these IROFS ~~controls~~ have high risk significance. The uncontrolled risk index will be used by the reviewer(s)~~staff~~ to identify all risk-significant [Comment: for consistency with the Rule terminology recommend changing "sets" to "system".] systems of IROFS~~sets of controls~~. These systems of IROFS~~sets of controls~~ will be reviewed with greater scrutiny than IROFS~~controls~~ established to prevent or mitigate accident sequences of low risk.