APPENDIX A

EXAMPLE PROCEDURE FOR ACCIDENT SEQUENCE EVALUATION

The appendix describes to the NRC reviewer, a method for reviewing 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-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, such that the performance requirements of 10 CFR 70.61 are met. 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 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 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**
Consequence Category 3: High	*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	
Consequence Category 2: Intermediate	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 Appendix B 10 CFR Part 20
Consequence Category 1: Low	Accidents of lesser radiological and chemical exposures than those above in this column	Accidents of lesser radiological and chemical exposures than those above in this column	Radioactive releases producing effects less than those referenced above in this column

* RD = Radiological Dose

** CD = Chemical Dose

Likelihood

10 CFR 70.61 also specifies the permissible likelihood of occurrence of accident sequences of different consequences. High-consequence accident sequences must be "highly unlikely" and intermediate-consequence accident sequences must be "unlikely." Implicitly, accidents in the low-consequence category can have a likelihood of occurrence less than “unlikely,” or simply "not unlikely." The likelihood of occurrence limits of 10 CFR 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"

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 whose consequences and likelihoods yield an unacceptable risk index and for which IROFS will have to 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 Cat. 3 High (3)	Acceptable Risk 3	Unacceptable Risk 6	Unacceptable Risk 9
Consequence Cat. 2 Intermediate (2)	Acceptable Risk 2	Acceptable Risk 4	Unacceptable Risk 6
Consequence Cat. 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 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 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 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)**

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 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, 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: 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) total effective dose equivalent (TEDE), or (b) chemical exposures that could endanger life (above AEGL-3 or ERPG-3); or (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). 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: An accident 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, or (b) chemical exposures that could lead to irreversible or other serious long-lasting health effects above AEGL-2 or ERPG-2); or (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), or (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: 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.

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

	Workers	Offsite Public	Environment
Consequence Category 3: High	*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	
Consequence Category 2: Intermediate	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
Consequence Category 1: Low	Accidents of lesser radiological and chemical exposures than those above in this column	Accidents of lesser radiological and chemical exposures than those above in this column	Radioactive releases producing effects less than those referenced above in this column

* RD - Radiological Dose
**CD - Chemical Dose

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

A.3 LIKELIHOOD CATEGORY ASSIGNMENT

An assignment of an accident sequence to a likelihood category is acceptable if it is based on the record of occurrences at the facility, the record of failures of safety controls at the facility or 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 judgement 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 to assign 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., 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 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 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. A summary of the risk index calculation will be given below.

Accident sequences result from initiating events, followed by failure of one or more IROFS. Thus there are columns, in Table A-7, 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." 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 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 second IROFS 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, 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 the 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.

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 (Red. 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 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.

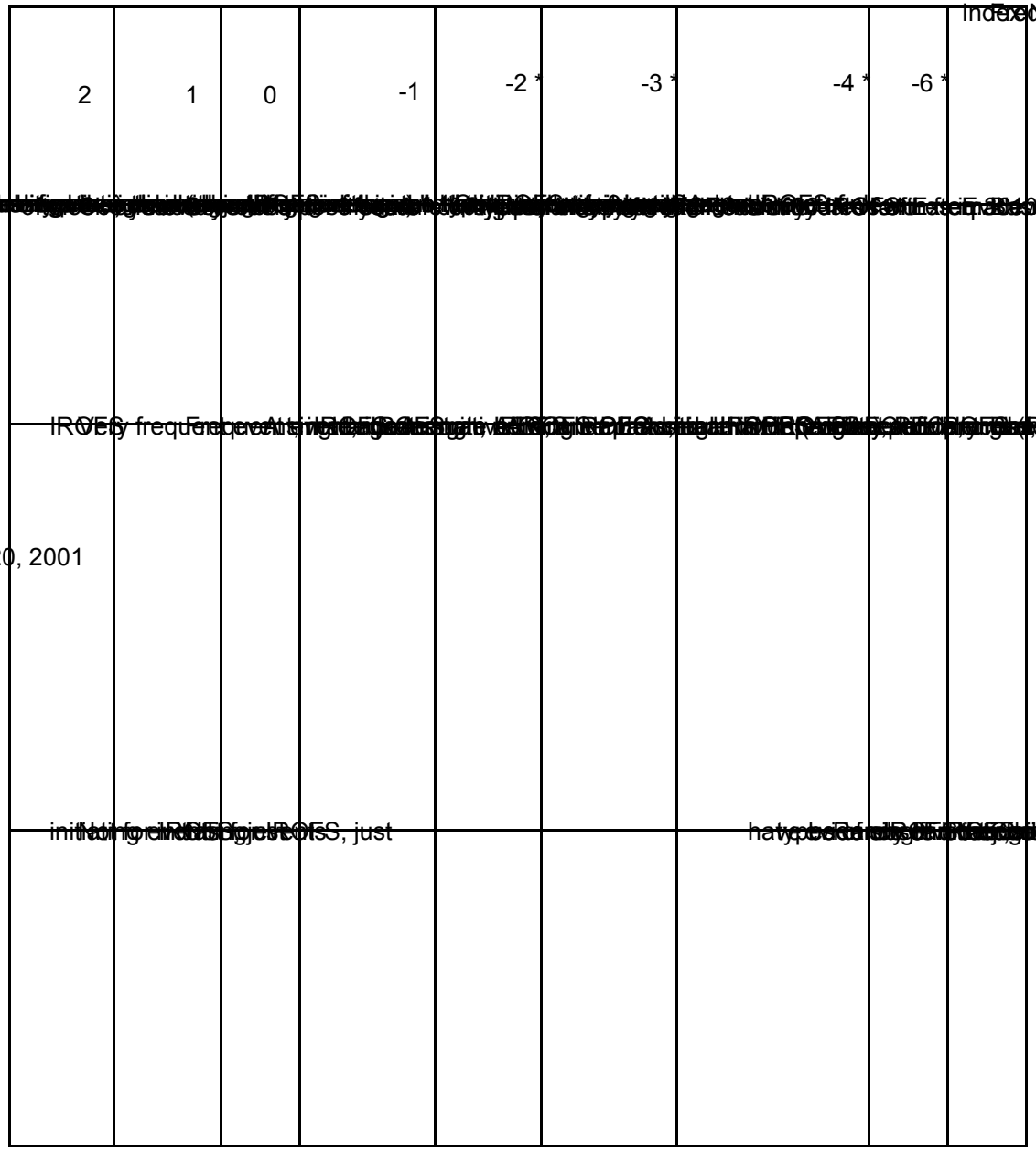

Table A-9: Failure

DRA

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

Table A-11: Failure Duration Index Numbers

-1 or -2	-2 or -3*	-3 or -4*	4 or -5* -6*	Probability Index No.
Probability of Failure on Demand	10^{-1} – 10^{-2}	10^{-2} – 10^{-3}	10^{-3} – 10^{-4}	10^{-4} – 10^{-5} 10^{-6}
Comments				

Table A-10: Fai

Based on Type of IROFS

DRA

DRA

Table A-12: Accident Sequence Descriptive List of Items Relied on for Safety

Accident (see Table A-6)	Description
PPB2-1A Blender UO_2 leak criticality	The initial failure is a blander 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 falls during cleanup or is not working, unmitigated consequences occur.
PPB2-1C	The events of PPB2-1 A 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-13 Descriptive List of Items Relied on for Safety

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

DRA

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 as 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 directly 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 as 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 non-redundant 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 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 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 a tabular summary of IROFS 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 IROFS and its 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, a history may exist 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

DRA

state when de