APPENDIX A
EXAMPLE PROCEDURE FOR RISK EVALUATION

NRC requirements in proposed 10 CFR 70.61 require that the occurrence of consequences of concern, defined in proposed §70.61 be sufficiently unlikely. In addition, proposed 10 CFR 70.62(c) requires that the applicant perform an Integrated Safety Analysis (ISA) to identify all potential accident sequences and to assess their consequences. These two requirements are related. The consequences of concern result from accident sequences identified in the ISA. Thus, to show that the likelihood of occurrence of the consequences is sufficiently low, the applicant must show that for each of the accident sequences identified in the ISA, the resulting consequences are sufficiently unlikely.

As defined in proposed 10 CFR 70.61, the required likelihood is graded according to the severity of the consequences of the accident. Accidents in the intermediate consequence category of proposed §70.61(c) must be "unlikely," while those in the high consequence category of proposed §70.61(b) must be "highly unlikely." The procedure described in this appendix is one way by which the applicant may use the ISA results to demonstrate that the requirements of proposed 10 CFR 70.61 have been met. If the applicant 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. The method requires the applicant to identify and evaluate the characteristics of controls used to limit accident sequences in a consistent manner. 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 safety controls must fail for consequences of concern in proposed 10 CFR 70.61 to occur. Chapter 5.0 specifies acceptance criteria for these safety controls, such that the performance requirements of proposed §70.61 are met. These criteria require that safety controls be sufficiently unlikely to fail. However, the criteria of Chapter 5.0 do not provide for a method for assessing likelihood. This appendix describes an acceptable procedure for this required assessment of likelihood.

A1. DETERMINING COMPLIANCE WITH GRADED PROTECTION REQUIREMENTS

Proposed 10 CFR Part 70.61 describes requirements for a graded system of protection sufficient to bound the risk of identified accidents by making accidents of higher potential consequences have a proportionately lower likelihood of occurrence. The regulation specifies two categories of consequences of concern into which an accident may fall. The first category is referred to in proposed §70.61 as "high consequences," the second as "intermediate consequences." Implicitly there is a third category, namely, those accidents that produce consequences less than "intermediate." These will be referred to as "low consequence" accidents. Since the primary purpose of process hazard analysis is to

identify all accidents having consequences of concern, it will, in some cases, be necessary to identify accidents that produce radioactive or chemical exposures, then subsequently determine that some of these exceed the threshold values of the regulation. For this reason, the list of accidents resulting from such analysis will include such low consequence accidents in order to show that they have been considered. Otherwise, the analysis will not have demonstrated its completeness.

The limits defining the three accident consequence categories are given in Table A-1. 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 symbols CHEM3, CHEM2, and CHEM1 refer to quantitative standards selected by the applicant in accordance with proposed 10 CFR 70.61(b)(4)(ii), 70.61(c)(4)(ii) –*e.g.*, AEGL or ERPG, as appropriate.

Consequence Category 3--High Consequences: An accident resulting in any consequence specified in proposed §70.61(b); that is: an acute worker exposure of 1 Sv (100 rem)[1] or greater TEDE[2], or a chemical exposure that could endanger the life of a worker (as defined by the applicant); or acute exposure of a member of the public outside the controlled area to a radiation dose (D) of 0.25 Sv (25 rem) or greater TEDE, a 30 mg soluble uranium intake, or a chemical exposure that could lead to irreversible or other serious long-lasting health effects, as defined by the applicant (represented herein as CHEM3).

Consequence Category 2--Intermediate Consequences: An accident resulting in any consequence specified in proposed §70.61(c). That is, acute exposure of a worker to a radiation dose of 0.25 Sv (25 rem) or greater but less than 1 Sv (100 rem) TEDE, or chemical exposure that could lead to irreversible or other serious long-lasting health effects, as defined by the applicant (represented herein as CHEM2); or acute exposure of a member of the public outside the controlled area to a radiation dose 0.05 (5 rem) or greater but less than 0.25 Sv (25 rem) TEDE, or a chemical exposure that could cause mild transient health effects, as defined by the applicant (represented herein as CHEM1); or 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 consequence Categories 3 and 2 above.

---

[1]A nuclear criticality would normally be considered a high consequence event because of the potential for producing a high radiation dose to a worker.

[2]TEDE is Total Effective Dose Equivalent (see 10 CFR Part 20), represented by ‘D’.

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

	Workers	Offsite Public	Environment
Consequence Category 3: high	$D^2 \geq$ 1 Sv (100 rem) $\geq$ CHEM3	D $\geq$ 0.25 Sv (25 rem) 30 mg sol U intake $\geq$ CHEM2	
Consequence Category 2: intermediate	0.25 Sv $\leq$ D < 1 Sv $\geq$ CHEM2 but < CHEM3	0.05 Sv $\leq$ D < 0.25 Sv $\geq$ CHEM1 but < CHEM2	radioactive release > 5000 x Table 2 App B 10 CFR 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 the rule (Categories 2 and 3 above), proposed §70.61 requires corresponding levels of graded protection, that is, engineered or administrative controls (or a combination thereof), sufficient to ensure that the likelihood of these adverse events is correspondingly low. The two categories of likelihood thus prescribed are:

Likelihood Category 1: Consequence Category 3 accidents must be "highly unlikely;" and

Likelihood Category 2: Consequence Category 2 accidents must be "unlikely."

Implicitly there is a third category into which an accident could fall, that is it could fail to be "unlikely." This category will be referred to in this document as:

Likelihood Category 3: "Not unlikely."

Although this likelihood 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.

Per proposed §10 CFR 70.61, the applicant must use the ISA is to document its compliance with the performance requirements. This evaluation should be done using a tabular summary of identified accident sequences. One acceptable way of doing so is for the applicant to assign two category numbers to each accident sequence, one based on its consequences and 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 acceptable. 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 proposed 10 CFR 70.61. This system is equivalent to assigning each accident to a cell in a 3 by 3 matrix. This conceptual matrix is shown in Table A-2. The values in the risk matrix cells are the risk index numbers.

TABLE A-2: Risk Matrix

	Likelihood Category 1: highly unlikely	Likelihood Category 2: unlikely	Likelihood Category 3: not unlikely
Consequence Cat. 3 High	3 acceptable	6 unacceptable	9 unacceptable
Consequence Cat. 2 Intermediate	2 acceptable	4 acceptable	6 unacceptable
Consequence Cat. 1 Low	1 acceptable	2 acceptable	3 acceptable

To demonstrate compliance with the system described above, the applicant needs to assign consequence categories to each identified accident in order to determine which likelihood requirement applies. Then those accident sequences identified as high or intermediate consequences must be assigned to a likelihood category. To be acceptable, these assigned consequences and likelihoods must have a valid basis, and the applicant must demonstrate this basis in the documentation submitted in the application. The following sections describe an acceptable method for making these assignments.

A2. CONSEQUENCE CATEGORY ASSIGNMENT

The assignment of consequence categories is based on estimated consequences of prototype accidents. Criteria for the presentation of these estimates by the applicant is described in Section 5.4.3.2(B)(iv). Although consequences of accidents can be determined by actual calculations, it is not necessary that such a calculation be performed for each individual accident sequence listed. Accident consequences may be estimated by comparison to similar events for which reasonably bounding conservative calculations have been made. The applicant should document the bases for bounding calculations of the consequence assignment in the submittal. NUREG/CR-6410, "Nuclear Fuel Cycle Facility Accident Analysis Handbook," describes valid methods and data to be used by the applicant and may be used for confirmatory evaluations by the reviewer.

A3. LIKELIHOOD CATEGORY ASSIGNMENT

An assignment of an accident sequence to a likelihood category is acceptable if it is based on the record of failures at the facility or other methods that have objective validity. Failure data from other facilities may also be used, but care should be taken to ensure its applicability. Because the sequences leading to accidents often involve multiple failures, a combination of failure frequency and probability values determines the likelihood of the whole accident sequence. These values include the frequencies of initiating events and failure likelihoods of safety controls. As described below, the applicant may estimate an approximate likelihood category for an accident sequence by considering all the events involved. This method uses the number, type, independence, and observed failure history of safety controls. However, correctly evaluating the appropriate likelihood of accidents using such a qualitative approach depends on the informed judgement of the analyst. Safety 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 likelihood of failure of safety controls involved is sufficiently low so that the entire accident sequence is "highly unlikely" or "unlikely" as required by proposed 10 CFR 70.61. The virtue of the approach is that it requires explicit consideration of some of the underlying events and factors that affect the likelihood of the accident. Another virtue is that the more explicit the criteria for assignment are, the more consistent are the results.

Underlying any evaluation of an accident sequence as "unlikely" or "highly unlikely" is an implied assessment of its "likelihood" or frequency of occurrence. The structured procedure described below will indicate which likelihood category may be appropriate for an event. In order to maintain internal consistency in evaluating different control systems and accidents, it was necessary to derive this structured procedure based on the underlying frequencies of events. The following numerical guidelines were thus used to obtain consistency:

Likelihood Category 1: Highly unlikely, a frequency of less than 10^{-5} per year per accident;

Likelihood Category 2: Unlikely[3], a frequency of less than 4×10^{-4} per year per accident (but more frequent than 10^{-5}); and

Likelihood Category 3: Not unlikely, more frequent than 4×10^{-4} per year per accident

In assigning specific numerical values to these likelihood categories, we are making definitive assumptions about the number of accident sequences. The Commission's

[3]A distinction must be drawn between the concept of "unlikely" in regard to intermediate consequence events and "unlikely" in regard to the double contingency principle. The above definition of unlikely does not apply to a nuclear criticality (which should be regarded as a high consequence event in unshielded facilities in most instances). In meeting double contingency, unlikely typically means $\leq 10^{-2}$.

strategic goals are stated in terms of total industry risk, so that the per accident probabilities must be expressed as the cumulative likelihood divided by the total number of accident sequences. For the purposes of this example, it will be assumed throughout the remainder of this appendix that there are 100 intermediate consequence accidents and 1000 high consequence accidents across the industry (this is consistent with SRP Section 5.4.3.2).

With this assumption, each individual accident sequence in this likelihood category should have a frequency no greater than 10^{-5} per year (i.e., one accident of this type every 100,000 years). This number can be multiplied by the total number of accident sequences to give the cumulative likelihood of all accident sequences in a given category at the facility, in units of yr^{-1}.

In assessing the adequacy of safety controls, individual accident frequencies greater than 10^{-5} per year may not be assigned a likelihood Category 1, that is, "highly unlikely." The NRC has a strategic safety performance measure of no inadvertent nuclear criticalities. For this reason, the acceptability of any given frequency depends on the total number of accidents that may be identified. Since the total number and consequences of all potential accidents at a facility is not accurately known until its ISA is completed, it is difficult to establish a definitive acceptable frequency. Individual accidents may need to be limited to lower frequencies to meet the performance requirements. On the other hand, the fact that a particular accident sequence is below this value does not automatically mean that it is clearly acceptable. The frequencies should be used as a guideline in developing more consistent and objective standards for safety goals. These likelihoods may be derived by considering the Commission goal that there should be no accidental criticalities at any regulated facility.

As an example, the value of 10^{-5} per year per accident in a facility with 100 potential accident sequences (Consequence Category 3) would yield a cumulative frequency for Consequence Category 3 accidents of:

$$100 \text{ accidents} \times 10^{-5} \text{ per year per accident} = 10^{-3} \text{ per year.} \qquad \text{(Eq. A-0)}$$

These Category 3 accidents generally result in fatalities. The average statistic for all manufacturing industries is that a facility with 250 manufacturing workers would expect 10^{-2} on-the-job deaths per year (see References, Statistical Abstract of the U.S.). The number of 10^{-3} per year is consistent with the Commission goal that there should be no accidental criticalities at regulated facilities. With approximately 10 regulated facilities in the United States, this should ensure that the likelihood of an accidental criticality anywhere in the country is no greater than 10^{-2}. A recurrence period of 100 years is sufficient to provide reasonable assurance that a criticality accident will not occur during the lifetime of any regulated facility.

Similarly, accident sequences having frequencies more than 4×10^{-4} per year per accident are considered "not unlikely" (assuming on the order of 100 accident sequences of this type in the industry). Again this value should not be taken as a definitive criterion for

acceptability. It is a guideline value to assure consistency. It may need to be adjusted based on the numbers and severity of accidents. The rationale for the value $4x10^{-4}$ is that accidents of the corresponding severity, Consequence Category 2, are not common and should remain so. This is based on a Commission strategic goal, that there should be no increase in reportable radiation releases, as discussed in SRP Section 5.4.3.2(B)(ix). To achieve this, the product of this frequency per accident per year with the assessed number of potential accidents should provide adequate confidence that such accidents will not occur. Note again that these values of 10^{-5} and $4x10^{-4}$ are per year per accident.

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 be applied. The reason double contingency is needed is the fact that there is usually insufficient firm data as to the reliability of the control equipment and administrative control 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 require two independent controls. Inadequate controls can then be determined by observing their failure, without also suffering the consequence of a criticality. Even with double contingency, it is essential that each of the items relied on for safety (IROFS) be sufficiently unlikely to fail. This is so that, if one of the two items that establish double contingency is actually ineffective, criticality will still not be likely.

A4. RISK INDEX EVALUATION SUMMARY

As mentioned in Section A3, an acceptable way for the applicant to present the results of the ISA is a tabular summary of the identified accident sequences. Table A-9 is an acceptable format for such a table. This table lists several example accident sequences for a powder blender at a MOX facility. Table A-9 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 fault tree is another acceptable method of presenting the results. As shown by the example, for the purposes of documenting compliance with the double contingency principle, a fault tree provides a fuller description of the control systems, and the logical progression of the accident, than a tabular format can, and is thus considered the preferred method. Both of these methods will be presented in the tables which follow.

Accident sequences result from initiating events, followed by failure of one or more controls. Thus, there are columns in Table A-9 for the initiating event and for controls which may be mitigative or preventive. In most cases, the initiating event will be the failure of one of the preventive controls. There may also be accident sequences resulting from external events such as fires or earthquakes.

With redundant safety controls, and in certain other cases, there are sequences where an initiating event occurs that places the system in a vulnerable state. While the system is in

this vulnerable state, a safety control must fail in order 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 failure. For this reason, it is necessary to consider the duration of the vulnerable state and to assign it a duration index. The values of all index numbers for a sequence are added to obtain a total likelihood index, T. 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-3.

Table A-3: 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 in Table A-3 applies to the accident sequence of a whole and is used to assess the overall likelihood of the sequence, not the likelihood of individual controls used in meeting double contingency.

The values of index numbers in sequences are assigned considering the criteria in Tables A-4 through A-6. Each table applies to a different type of event. Table A-4 applies to events which have frequencies of occurrence, such as initiating events and certain control failures. When failure probabilities are required for the event, Table A-5 provides the index values. Table A-6 provides index numbers for durations of failure. These are used in certain accident sequences where two 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 susceptible to failure of the second. The reverse sequence, where the second control fails first, should also be considered as a separate accident sequence. (Since the example chosen concerns mainly criticality safety, the failure of each control relied on to meet the double contingency principle must be considered as the initiating event of an accident sequence.) This is necessary because the duration of failure of the second control will usually differ from that of the first. The values of these duration indices are not merely judgmental. They are directly related to the time interval of surveillance monitoring for failures. That is, the duration of a failure is the time until it is detected plus the time to restore the system to a state where it is not vulnerable to the second failure.

If the probability of failure for the first preventive control is P_1 (in units of events per yr), its duration of failure is d_1 (in years), and the probability and duration of failure of the second control is P_2 and d_2, then P_1P_2 is the probability that both controls will fail within the year. The probability that both controls will be in a failed state simultaneously is $P_1P_2(d_1+d_2)$. The two terms $P_1P_2d_1$ and $P_1P_2d_2$ correspond to the direct and reverse accident sequences (that

is, where Control 1 fails first followed by Control 2, and *vice versa*). Thus, we see that taking the duration index into account can produce a substantial reduction in the overall likelihood of the accident sequence.

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 (see Table A-1). Multiple types of consequences can result from the same event. The consequence category for an event is chosen for the most severe consequence.

As shown in the first row of Table A-9, 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 (about one month), to be acceptable, should be based on the intentional monitoring frequency of the process. The failure duration for an unmonitored process should be conservatively estimated.

Table A-7 provides a more detailed description of the accident sequences used in the example of Table A-9. The reviewer needs the information in Table A-7 to understand the nature of the accident sequences listed in Table A-9. Table A-9 lacks sufficient room to explain any but the simplest failure events.

Table A-8 is used to explain the safety controls and external initiating events that appear in the accident sequences in Table A-9. The reviewer needs the information in Table A-8 to understand why the initiating events and safety controls listed in Table A-9 have the low likelihood indices assigned. Thus, Table A-8 needs to address such information as: the margins to safety limits, the redundancy of a control, and the measures taken to assure adequate reliability of a control. Table A-8 must also justify why those external events, which are not obviously extremely unlikely, have the low likelihoods which are being relied on for safety. The applicant should provide separate tables to list the controls for criticality, chemical, fire, radiological, and environmental accidents.

Table A-4: Failure Frequency Index Numbers

FREQUENCY INDEX NUMBER	BASED ON EVIDENCE	BASED ON TYPE OF CONTROL**	COMMENTS
-6 *	External event with freq. < 10^{-6} per yr		If initiating event, no controls needed
-4 *	No failures in 30 yr for hundreds of similar controls in industry	Exceptionally robust passive engineered control (PEC), or an inherently safe process, or 2 independent active engineered controls (AECs), PEC, or enhanced admin. controls.	Rarely justified by evidence, since few systems are found in such large numbers. Further, most types of single control have been observed to fail.
-3 *	No failures in 30 yr for tens of similar controls in industry	A single control with redundant parts, each a PEC or AEC	
-2 *	No failure of this type in this facility in 30 yr	A single PEC	
-1	A few failures may occur during facility lifetime	A single AEC, an enhanced administrative control, an admin. control with large margin, or a redundant admin. control	
0	Failures occur every 1 - 3 yr	A single administrative control	
1	Several occurrences per yr	A frequent event	Not for safety controls, just initiating events
2	Occurs every week or more often	Frequent event, an inadequate control	Not for safety controls, just initiating events

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

** The failure frequency index assigned to a control of a given type in column 3 may be one value higher or lower than the value given in column 1, since the reliability of different types of controls can vary widely. Criteria justifying assignment of the lower (more negative) failure frequency index should be given in the narrative describing ISA methods. Exceptions should be individually justified.

Table A-5: Failure Probability Index Numbers

PROBABILITY INDEX NUMBER	PROBABILITY OF FAILURE ON DEMAND	BASED ON TYPE OF CONTROL	COMMENTS
-6 *	10^{-6}		If initiating event, no controls needed
-4 or -5 *	10^{-4} - 10^{-5}	Exceptionally robust passive engineered control (PEC), or an inherently safe process, or 2 redundant controls better than simple admin controls (active engineered control (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 controls have been observed to fail.
-3 or -4 *	10^{-3} - 10^{-4}	A single PEC or an AEC with high availability	
-2 or -3 *	10^{-2} - 10^{-3}	A single AEC, or an enhanced admin control, or an admin control for routine planned operations	
-1 or -2	10^{-1} - 10^{-2}	An admin control that must be performed in response to a rare unplanned demand	

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

Figure A-2 presents the same information as a set of fault tree diagrams. A discussion and comparison of the two methods follows the example.

Definitions and explanations of the terms used in the following tables and figures will follow the example.

As an understanding of the example systems is important, process descriptions for hypothetical MOX processes follow. These hypothetical systems were chosen because of their relatively high degree of importance for nuclear criticality and because they represent the extremes in terms of operational and control complexity. The first example, the solvent extraction system, is a complex chemical operation that is most amenable to a fault tree presentation of the results of the ISA summary (though to compare the strengths and weaknesses of the two methods, both fault trees and a tabular format are presented). The second example, mixed oxide blending, is much more straightforward in terms of controls and the results of the ISA can be summarized more effectively in terms of a table of accident sequences.

These examples should only be considered typical of the degree of information required and the ways in which it may be displayed. It is anticipated that the applicant's ISA Summary and process description may differ markedly from the example. These examples should not be construed to preclude other methods of presenting the ISA summary results.

A5. OVERALL PROCESS DESCRIPTION

The purpose of the front-end Plutonium Purification Process (P^3) is to remove impurities such as gallium and americium from the plutonium oxide feed, producing a more suitable plutonium feed stream for the oxide blending process. This process description is for illustrative purposes only and should not be expected to conform to any particular applicant's process. The actual license application would require a more detailed process description than that presented below, but the following brief summary is presented to aid in understanding the example:

Raw plutonium oxide (PuO_2) powder is received from the shipper and batched into a glovebox at the front end of the Aqueous Polishing (AP) processing line. The containers of PuO_2 are fed into an electrically-heated dissolver unit in the glovebox, consisting of a favorable geometry recirculation loop with electrodes at either end. The PuO_2 is digested by the addition of nitric acid in the presence of Ag^{++} ions, resulting in the formation of an impure plutonium nitrate ($Pu(NO_3)_4$) solution at a concentration of ~250 gPu/l. Plutonium can exist in several oxidation states in nitric solutions simultaneously, which complicates the process chemistry considerably. Although the plutonium in PuO_2 is tetravalent (Pu(IV)), it undergoes disproportionation, or self-oxidation and reduction, to both Pu(III) and Pu(VI) through the reaction

$$3Pu^{4+}\ (IV) + 2H_2O \rightleftarrows 2Pu^{3+}\ (III) + PuO_2^{2+}\ (VI) + 4H^+ \qquad \text{(Eq. A-1)}$$

Table A-6: Failure Duration Index Numbers

DURATION INDEX NUMBER	AVG. FAILURE DURATION	DURATION IN YEARS	COMMENTS
-5	5 minutes	10^{-5}	
-4	1 hour	10^{-4}	
-3	8 hours	0.001	
-2	A few days	0.01	
-1	One month	0.1	Formal monitoring to justify indices less than "-1"
0	One year	1	
1	More than 3 years	10	

The plutonium must be adjusted to the tetravalent state to ensure effective extraction. This is done as a two-step process. First, Ag^{++} is generated at the cathode and acts as an oxidation agent to drive both Pu(III) and Pu(IV) to Pu(VI). Tetravalent plutonium is oxidized through the reaction Pu(IV) + $Ag^{++} \rightleftarrows$ Pu(VI) + Ag.

After the operators determine that complete PuO_2 dissolution is achieved by means of independent dual sampling, the $Pu(NO_3)_4$ is fed through a favorable geometry in-line filter into the solvent extraction feed preparation slab tank. (*N.B.* Plutonium in $Pu(NO_3)_4$ is actually in the tetravalent state; the chemical form after oxidation is more accurately characterized as a mixture of Pu(VI) cations in a NO_3^- -rich solution.) The free Pu(VI), or PuO_2^{+2} plutonyl ions, must be adjusted from the hexavalent to the tetravalent state Pu(IV) by the addition of excess HNO_3 and H_2O_2 (a reducing agent) at a low plutonium concentration. This is done in the favorable geometry preparation tank. The entire aqueous polishing process is conducted on a batch basis, with approximately 14 kg (30.8 lb) Pu processed through dissolution, solvent extraction, precipitation, and calcination in each batch. The powder is then mixed together with natural uranium oxide to form the master blend.

A6. SOLVENT EXTRACTION PROCESS (PLUTONIUM PURIFICATION)

The Solvent Extraction, Scrub, and Strip columns consist of identical long (~20 feet [6.1 m]), 5-inch (12.7 cm) diameter Pyrex columns containing a series of stationary perforated plates. For solvent extraction, the aqueous $Pu(NO_3)_4$ solution is added at the top of the column and a mixture of TBP, or tributyl phosphate (chemical formula $(C_4H_9)_3PO_4$), and a diluent (30% hydrogenated tetrapropylene, or HTP) is added at the bottom of the column. The difference between the relative specific gravities of the two streams causes the aqueous solution to sink to the bottom and the organic mixture to rise to the top of the column. The immiscible fluids are pulsed in the columns by means of positive-displacement pumps. This pulsing breaks up the interface between the fluids and increases the surface area, resulting in intimate mixing to increase the efficiency of extraction. The tetravalent plutonium ion Pu^{4+} becomes complexed to the organic through the reaction:

$$Pu^{4+}(aq) + 4NO_3^-(aq) + 2TBP(o) \rightleftarrows Pu(NO_3)_4 \cdot 2TBP(o) \qquad \text{(Eq. A-2)}$$

The existence of a salting agent such as HNO_3 or $Al(NO_3)_3$ increases the acid molarity of the excess nitric ion, and causes the above reaction to be shifted to the right.

In the scrub column, the fissile-bearing organic stream from the top of the solvent extraction column is fed into the bottom of the scrub column. Additional nitric acid is added to the top of the scrub column and the same countercurrent operation repeated, to remove additional impurities from the organic into the aqueous phase. The plutonium remains in the organic phase at the end of the scrub operation. The aqueous *raffinate* stream–which should now contain low levels of plutonium but concentrated fission products–is transferred to raffinate storage while the fissile-bearing organic stream fed into the bottom of the strip column.

In the strip column, deionized water is added to reduce the acid molarity, causing the left hand side of Equation A-2 to be favored. The aqueous product stream containing purified plutonium nitrate is then transferred to the first pass evaporator; the spent organic phase must be reconditioned for reuse in the first pass solvent extraction. The evaporator consists of a tube-and-shell heat exchanger in which the concentration of the $Pu(NO_3)_4$ increases from 40 gPu/l to around 250 gPu/l. The second and third pass solvent extraction lines are nearly identical to the first, except that the $Pu(NO_3)_4$ is at a higher concentration.

Raffinate and solvent conditioning streams attach to the process at various points. The first, second, and third pass raffinate streams are transferred to a bank of favorable geometry columns (from the extraction and scrub columns, solvent regeneration, and evaporator condensate), where they are sampled (by dual independent sampling) for Pu content. Only after they meet the release criteria of 0.015 gPu/l are the contents discharged (through an in-line monitor that is interlocked to the waste tank isolation valves) to a set unfavorable geometry waste water tanks, for waste water treatment and eventual discharge from the site. In addition, organic solvent from the strip columns must be regenerated because it contains a build-up of metallic impurities (primarily gallium and americium), nitric acid (acquired through the reaction $H^+(aq) + NO_3^-(aq) + 2TBP(o) \rightleftarrows HNO_3 \cdot TBP(o)$), and various radiolytic decomposition products of TBP and kerosene, such as dibutyl phosphate (DBP). The solvent is washed with Na_2CO_3, NaOH, and HNO_3 in a series of favorable geometry Mixer/Settlers (M/Ss) to remove impurities, filtered, and recycled to the solvent extraction columns. Gallium and americium is further removed by electrolytic deposition on charged plates in the M/S units. Makeup solvent from bulk chemical tanks is added as needed to maintain the solvent inventory. The M/Ss consist of a safe geometry box partitioned by a short wall into a mixing chamber and a settling chamber. The mixing chamber contains a rotary impeller which draws the heavier liquid (aqueous wash solution) from the bottom of the mixing chamber and emulsifies it into the lighter liquid (organic solvent) in the top of the mixing chamber. Following this intimate mixing (which operates under the same principle as the pulsed extraction columns), the solution gravity drains into the settling chamber, where it separates into two distinct layers. The organic is drawn off to the next wash stage or to the fresh solvent column, while the aqueous is discharged to the raffinate storage columns.

Following third pass solvent extraction, the purified $Pu(NO_3)_4$ must be re-converted to PuO_2 for blending with UO_2. This is accomplished by the addition of oxalic acid ($H_2C_2O_4$) to cause the precipitation of plutonium as plutonium oxalate ($Pu(C_2O_4)_2$). Hydrogen peroxide (H_2O_2) is added to the plutonium nitrate solution to ensure that it is in the proper oxidation state. After sampling, the solution is transferred to the precipitation column, a short 4-inch (10.2 cm) diameter glass column contained within a glovebox, in which the plutonium oxalate is prepared. Precipitation proceeds through the reaction:

$$Pu(IV)(NO_3)_4 + 2H_2C_2O_4 \rightleftarrows Pu(C_2O_4)_2 + 4HNO_3 \qquad \text{(Eq. A-3)}$$

The resulting precipitate is prepared through the slow addition of oxalic acid to the column, and is thixotropic in nature. The nitric acid content must also be adjusted to obtain the desired level of consistency. The resultant plutonium oxalate slurry collects at the bottom of the column. The residual nitric-water solution contains only low levels of plutonium

nitrate and is sampled for discharge. Solutions which contain greater than the release criteria of 0.015 gPu/l are recycled to solvent extraction for re-extraction. This dilute nitric solution is decanted and filtered before transfer to acid recovery, and the material at the bottom of the bowl drained out before being air-dried in the glovebox. When the material is dried, it forms a cake containing plutonium oxalate hydrates (such as $Pu(C_2O_4)_2 \cdot 6H_2O$). The material is gravity drained from the bottom of the precipitator, where it is automatically dropped through a chute into an inclined, rotary-kiln calciner in a continuous process. The slurry is then calcined in an electrically heated oxidation furnace at 300 °C and then converted to PuO_2 at 900 °C in an oxygen-rich atmosphere in the same furnace. The PuO_2 is collected into a moderation-controlled hopper, which is connected to a favorable geometry tumbling mixer to achieve proper homogenization. The mixer consists of two rotating drums with a spiral blade in the intervening space with a cadmium shaft for neutron poison. After homogenization, the material is transferred to a glovebox where it is sampled, bottled, and transferred to the Mixed Oxide Blending Operation of the MOX Process (MP) Line.

The overall process flow is shown in Figure A.1.

Controlled parameters in the solvent extraction process are geometry, concentration, spacing, interstitial moderation, and process variables (material form). The solvent extraction columns were modeled using an optimal plutonium nitrate concentration of--140 GPU/l, without taking credit for the presence of gallium –a mild neutron poison–-or excess nitric acid. The solution was modeled to the outer diameter of the columns, and thus took credit for the diameter but not the column thickness. Credit was not taken for the plutonium isotonic (~4wt% ^{240}Pu), as the models assume the feed consists solely of ^{239}Pu. Concentration was not controlled for the extraction columns, but was credited for keeping the waste tanks subclinical upon solution transfer from the refined storage columns.

Because the design relies primarily on passive engineered features (*i.e.*, fixed geometry and spacing), the potential for nuclear criticality in the solvent extraction system itself is extremely unlikely. The main accidents of concern are transfer of concentrated solution to unfavorable geometry process equipment. As shown in Figure A-1, the unfavorable geometry systems that are connected to the process consist of (i) steam supply for the evaporators, (ii) demonize water, nitric acid, and solvent regeneration bulk chemical supply tanks, (iii) waste water system tanks, and (iv) the floor.

The example shown in the following tables is for the second pass solvent extraction (2SX) in the P^3 Process Node. The list of accident sequences and controls is for illustrative purposes only and is not meant to be exhaustive.

1. PROCESS CRITICALITY FLOW DIAGRAM

   Figure A-1 is an example of one method of describing the process flow. A good understanding of the process flow and the criticality control systems that exist at each node in the process is essential to evaluating the results contained in the ISA Summary. The information contained in this Process Criticality Flow Diagram (PCFD) is a more condensed form of the information that would be expected in the process

description, process flow diagrams (PFDs), and criticality safety evaluations. Presenting the information in this way is advantageous to the applicant, as it is a more efficient means of providing needed process knowledge to the ISA or safety discipline reviewer. Basically, the PFD. is a PFD modified to contain the features relied on for criticality safety. Note several useful features of this diagram:

The different process steps are divided into two categories by shape, those relying on favorable geometry and those which are unfavorable geometry. Distinguishing between these two types of systems may be done by several other means. Geometry control is typically ranked as the most preferable control due to its inherent stability and robustness, and is the primary control relied on in most of this particular system. In certain other systems, it may be somewhat more advantageous to draw a distinction between process steps that are moderation controlled and uncontrolled areas, or between concentration controlled and uncontrolled areas. By reviewing this diagram, it is immediately apparent where the transition from favorable to unfavorable geometry takes place.

Another feature of this diagram is that the engineered features relied on for criticality safety are clearly identified by shading. There is a simple graphic representation of the barriers that exist between favorable and unfavorable geometry equipment, which are drawn as bars across the flow path between these systems. This makes it readily apparent what features prevent the backflow of concentrated fissile solution to unfavorable geometry equipment, among other scenarios. Adding the labels that correspond to each of the IROFS (as in Table A-8) would provide a ready cross-reference, but may result in too much added complexity for such a system.

The use of different line patterns to distinguish between the various streams–particularly with respect to different fissile compositions–facilitates understanding of the process flow. Another useful feature is the division of the entire diagram into different zones corresponding to various process nodes. This provides a clearer boundary definition and allows the review to see how the system functions together as an integrated whole, including how perturbations in criticality controls in one process node or piece of equipment flows down into the next. The engineered controls tabulated in the ISA Summary (such as Table A-8) should include all features relied on for safety within the boundary of that process node. Finally, this diagram displays the actual controlled parameters at each process step; to the degree possible, this should be extended to display the actual controlled values of those parameters.

This diagram should be consulted in reviewing the sample tables.

Figure A-1: Criticality Flow Diagram for P [3] Operation

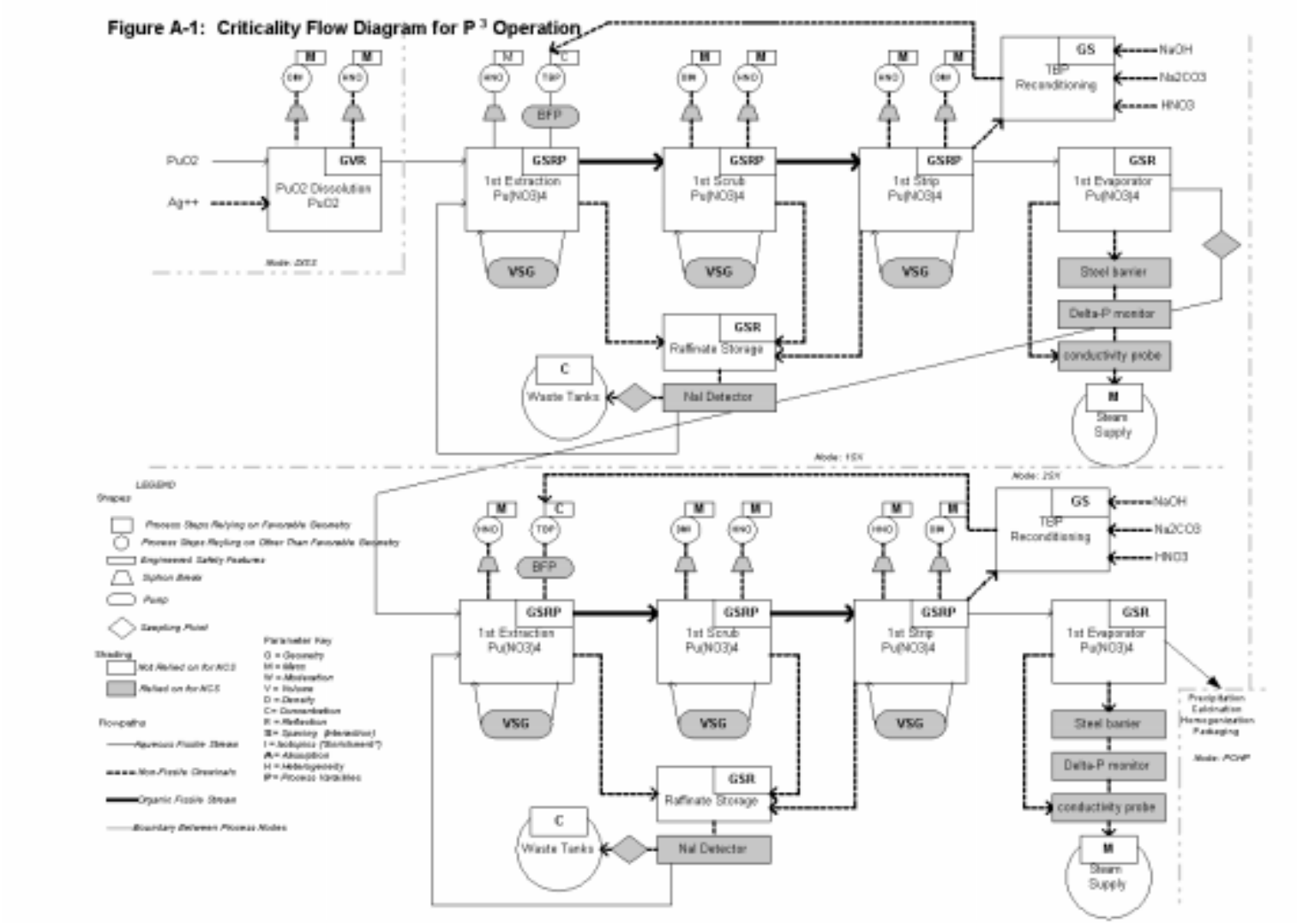


Table A-7: Accident Sequence Descriptions

Accident Sequence (see Table A-9)	DESCRIPTION
Loss of MASS	
MOB-001	Exceeding the mass limit of the blend tank, by adding too much UO_2 blendstock. This will have the effect of increasing the overall mass present, but will simultaneously decrease the plutonium "enrichment." The overall effect of this is to increase the distance from the subclinical curve of mass as a function of plutonium "enrichment" as more blendstock is added. The system is adequately subclinical under conditions of double batching uranium. To achieve criticality, this would have to be followed by a loss of moderation control.
MOB-002	Exceeding the mass limit of the blend tank, by adding too much PuO_2. This will have the effect of increasing both the overall mass and plutonium "enrichment." At ~33 kg PuO_2 (73 lb) (and 23 wt%) the subclinical mass limit will be exceeded. Therefore, this could lead to criticality without any additional upsets and therefore dual controls are established on the plutonium mass.
MOB-003	Exceeding the mass limit of the blend tank by performing the blending operation while there is still blended oxide present from the previous batch in the tank. Assuming the previous batch was properly mixed, it would require an additional 50 kg (110 lb) of PuO_2+UO_2 to exceed the subclinical mass limit. Therefore this could lead to criticality without any additional upsets and therefore dual controls are established to ensure the blend tank is empty of material before another batch is started.
Loss of MODERATION	
MOB-004	Exceeding the moderation limit (1wt% H_2O) by adding UO_2 which has not been properly sampled. This could lead to criticality without any additional failures. Dual independent sampling is required to ensure moisture limits are adhered to. Also, material will not freely flow through orifice if wet.
MOB-005	Exceeding the moderation limit (1wt% H_2O) by adding PuO_2 which has not been properly sampled. This could lead to criticality without any additional failures. Dual independent sampling is required to ensure moisture limits are adhered to. Also, material will not freely flow through orifice if wet. In addition, both the plutonium feed hopper and blend hopper are heated. Material is added at a sufficiently slow rate that contact with the heated blendstock will cause moisture in the plutonium to be driven off.
MOB-006	Exceeding the moderation limit (1wt% H_2O) by introduction of liquid water from overhead water lines or roof leaks. The blend tank is completely enclosed within an airtight and watertight enclosure. There are no overhead water lines allowed. The most likely cause of this scenario is backflow of condensate from the ventilation header, which serves to remove evolved water from the heated material. The ventilation header is sloped and equipped with drain lines to ensure against condensate backflow. Even in the event of water intrusion, the heating is sufficient to drive off any realistic accumulation of liquid water.
Loss of PLUTONIUM "ENRICHMENT"	
MOB-007	Exceeding the plutonium "enrichment" by adding too little blendstock to the blending hopper. This will have the effect of increasing plutonium "enrichment" while decreasing the overall mass. This will eventually reach criticality without any additional failures, by only when more than half the original UO_2 blendstock is omitted.
MOB-008	Exceeding the plutonium "enrichment" by adding too much PuO_2 feed to the blending hopper. This is identical to Scenario MOB-002 and will be discussed as a loss of mass control.
MOB-009	Exceeding the plutonium "enrichment" by adding PuO_2 to the blending hopper without first adding blendstock. This is the bounding case of Scenario MOB-007. Controls are established to ensure that blendstock is added and in the correct proportion before addition of PuO_2 feed is allowed.

Accident Sequence (see Table A-9)	DESCRIPTION
MOB-010	Exceeding the plutonium "enrichment" by the formation of clumps of higher enrichment PuO_2 in the blending hopper. Clumping can be caused by I) too high a plutonium feed rate, ii) failure of the magnetic stirrer, iii) failure of the deflection plate, or iv) failure of moderation control, resulting in a more cohesive mix. Calculations show there are sufficient controls such that homogeneity is not necessary to ensure subcriticality. However, criticality could occur if clumping were followed by a loss of moderation control.

2. DETERMINATION OF LIKELIHOOD CATEGORY IN Table A-3

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.

3. DETERMINATION OF FAILURE FREQUENCY INDEX NUMBERS IN Table A-4

Table A-4 is used to assign frequency index numbers to facility initiating events and control system failures as found in the columns of Table A-9. The term failure must be understood to mean not merely failure of the control device or procedure, but also as violation of the safety limit by the process. In the example in Table A-9, accident sequence 2SX-001 involves loss of volume control due to pump failure. If criticality is the concern, failure does not occur unless an unsafe volume of uranium-oil mixture collects in the oil reservoir 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 control failures do not cause safety limits to be exceeded.

Table A-4 provides two columns with two sets of criteria for assigning an index value, one based on type of control, the other directly on observed failure frequencies. The types of controls are administrative, active engineered, passive engineered, etc. Since controls 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 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 Control," references to redundancy allow for controls 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 a comparable process elsewhere or in the licensed facility. Justification for specific assignments may be noted in the Comments column of Table A-9.

As previously noted, the definition of failure of a safety control to be used in assigning indices is, for non-redundant controls, a failure severe enough to cause an accident with consequences. For redundant controls, it is a failure such that, if no credit is taken for functionality of the other control, an accident with consequences would result. If most control 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 controls unless the configuration management, auditing, and other required management measures are of high quality, because, without these measures, the

controls may be changed or inadequately maintained. The reviewer should be able to determine this from a tabular summary of safety 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 control and its applied management measures.

4. DETERMINATION OF FAILURE PROBABILITY INDEX NUMBERS IN Table A-5

Occasionally, information concerning the reliability of a 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, the applicant must know the demand frequency, the initiating event, and the demand failure probability of the safety control. This table provides an assignment of index numbers for such controls in a way that is consistent with Table A-4. 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.

5. DETERMINATION OF FAILURE DURATION INDEX NUMBERS IN Table A-6

The failure duration index is important because of reasons discussed above–it represents the window of opportunity after failure of the first preventive control during which the failure of the second could lead to adverse consequences. Cases in which the loss of the first control may remain undetected for long periods of time (such as leakage of hidden or baffled piping when credited as primary containment, or failure of items only tested when challenged) will typically not credit the failure duration in reducing the probability of the accident scenario. In this case, the duration index *D* should be taken as 0. Duration indices less than -1 should be based on periodic surveillance and/or maintenance periods, or the fact that failure would be readily apparent within a certain time frame. For example, a failure duration index of -2 would be based on the fact that a weekly surveillance requirement has been established for that item. A failure duration index of -3 may be based on a requirement to perform a certain measurement once per shift, or the fact that failure would immediately reveal itself to operators who are required to be continually present.

Table A-8: Criticality Safety Limits and Controls

IROFS for the Second Pass Solvent Extraction system

IROFS Identifier	Parameters and Limits	IROFS Description	Management Measures	QA Grade
2SX-PE1	VOLUME: <4.5 L (1.2 gal)	SX Pump PMPX-001 has a safe volume chamber.	Configuration control	B
2SX-AE1	GEOMETRY: < 7.6 cm (3") depth	SX Pump PMPX-001 has an active level switch on the oil reservoir, which automatically shuts the recirculation valve and sounds an audible alarm in the control room if the slab depth is exceeded.	1. Configuration control 2. Control room constantly monitored. 3. Biweekly functional check.	A
2SX-AE2	PROCESS VAR: ΔP < 0.34 atm (5 psi)	Pressure differential gauge on heat exchanger HX-001 is set to alarm if P_{tube} - P_{shell} < 0.34 atm (5 psi).	1. Configuration control. 2. Control room constantly monitored. 3. Functional check each shift.	A
2SX-AE3	PROCESS VAR: not applicable.	Conductivity probe on heat exchanger shell side to detect intrusion of plutonium. Set point will be sufficient to detect a concentration of 0.1 GPU/l.	1. Configuration control. 2. Functional test weekly.	A
2SX-ADM1	PROCESS VAR: ΔP < -0.34 atm (-5psi)	Procedures require operator response to differential pressure gauge alarm.	1. SOP 5349 2. Training/postings.	B
2SX-PE2	MASS: 0 mass in nitric acid supply	Siphon break installed in nitric acid supply line.	1. Configuration control.	C
2SX-ADM2	MASS: 0 mass in nitric acid supply	Utility (in this case, nitric acid) supply gauges are continually monitored in the control room whenever fissionable material is being processed. Facility procedures require shut down when utility pressure lost.	1. SOP 9483 2. Training/postings.	B
2SX-PE3	MASS: 0 mass in DIW supply	Siphon break installed on Deionize Water (DIW) line.	1. Configuration control.	C
2SX-ADM3	MASS: 0 mass in DIW supply	Utility (in this case, DIW) supply gauges are continually monitored in the control room whenever fissionable material is being processed. Facility procedures require shut down when utility pressure lost.	1. SOP 6879 2. Training/postings.	A
2SX-ADM4	PROCESS VAR: Acid molarity —.	DIW must be added to reduce acid molarity in the strip column to < —M. This ensures the plutonium will be stripped back into the aqueous phase.	1. SOP 0292 2. Training/postings.	A
2SX-ADM5	CONCENTR: < 0.1 GPU/L in the solvent regeneration columns	Procedures require weekly check of solvent regeneration columns by dual independent sampling. In addition, at the start of each batch, a checklist requires operators to visually check the columns for observed plutonium intrusion (greenish color).	1. SOP1929 2. Training/postings 3. QA Lab procedure ensures independ.	B
2SX-PE4	MASS: 0 mass in bulk chemical supply	Backflow preventer (BFP) installed on bulk chemical and DIW lines to prevent backlog to organic solvent supply tanks.	1. Configuration control. 2. Annual surveillance.	B
2SX-PE5	GEOMETRY: diam < 10.2 cm (4")	Columns must be composed on no greater than 10.2 cm (4") diameter glass (extraction, scrub, strip, and precipitation).	1. Configuration control.	C
2SX-PE6	GEOMETRY: depth < 5.2 cm (2") Area > 4.65 ^{M2} (50 ft^2)	Catch pans beneath columns must be no more than 5.2 cm (2") deep. In addition, they must have an area of 4.65 ^{M2} (50 ft^2) or more to ensure that they are capable of handling the largest spill from the columns.	1. Configuration control.	C

IROFS Identifier	Parameters and Limits	IROFS Description	Management Measures	QA Grade
2SX-PE7	SPACING: columns > 61 cm (24") center-to-center	Drawings require columns be installed no more than 61 cm (24") center-to-center (c-to-c).	1. Configuration control.	C
2SX-ADM6	MODERATION: water not allowed in fighting fires	Facility emergency response procedures prohibit the use of water in fighting fires in the solvent extraction area, when plutonium is being processes. There is no automatic sprinkler system in this area. Foams and fogging agents may be used.	1. Emergency Plan. 2. Training/postings. 3. Annual drill. 4. Configuration control.	C
2SX-PE8	MODERATION: no overhead lines in SX area	Overhead water lines are prohibited in the solvent extraction area.	1. Configuration control.	C
2SX-PE9	GEOMETRY: width < 7.6 cm (3")	Width of the solvent regeneration M/Ss must be less than 7.6 cm (3").	1. Configuration control.	C
2SX-PE10	GEOMETRY: diameter < 7.6 cm (3")	Diameter of the floor drains must be less than 7.6 cm (3").	1. Configuration control.	C
2SX-PE11	GEOMETRY: depth < 2.54 cm (1")	Floor must be sloped to drain into the favorable geometry floor drains; variation in floor level must not allow solution more than 2.54 cm (1") deep to accumulate.	1. Configuration control. 2. Annual audit.	C
2SX-AE4	CONCEPT: < 0.015 GPU/L	In-line monitor interlocked to isolation valve, to terminate feed if concentration > limit. Safety grade items are the monitor, the interlock electronics, and the isolation valve.	1. Weekly calibration and functional source check. 2. Configuration control.	A
2SX-ADM7	CONCEPT: < 0.015 GPU/L	Dual independent samples must be drawn and confirmed before transfer of refined to the waste water tanks is permitted. The results of sampling must be reviewed by the operator and a supervisor (who maintains control of the key to the valve lock).	1. SOP 9045 2. QA Lab procedure 3. Training/postings	A
2SX-PE12	SPACING: columns > 61 cm (24") c-to-c	Structural supports must be designed to withstand credible loads with a safety factor ≥ 2. Must be designed to withstand seismic loads > —g.	1. Pre-startup load testing. 2. Configuration control.	C
2SX-ADM8	CONCEPT: < 0.015 GPU/L	Excess nitric added in extraction and scrub columns sufficient to maintain a pH of –. Needed to keep refined concentration at a sufficiently low level.	1. SOP 3934 2. Lab QA procedure	B
2SX-ADM9	CONCEPT: < 0.015 GPU/L	Concentration in second pass extraction limited to —GPU/L. Along with 2SX-ADM8, needed to ensure extraction efficiency to keep refined concentration sufficiently low.	1. SOP 0945 2. Lab QA procedure	B
2SX-ADM10	SPACING: containers > 30.5 cm (12") from columns	Facility procedures require that fissile material contains and portable equipment be maintained at least 30.5 cm (12") from columns and pumps. Reinforced by postings and blue lines painted on floor (Limited Movement Areas).	1. Supervisor walk-through shiftly. 2. Facility directive 07. 3. Training/postings.	C
2SX-ADM11	MAT'L FORM: oil < 4L (1.1 gal)	The amount of oil in the oil reservoir of any pump shall be limited to 4L (1.1 gal). This limits the concentration of hydrogenous moderators other than water to ensure subclinical calculations are bounding.	1. Configuration control.	C
2SX-ADM12	MAT'L FORM: no precipitating agents	Lids to bulk chemical supply tanks must be locked and controlled by supervisors, to ensure against the inadvertent addition of precipitating agents. Addition of all reagents must be certified by a facility chemical engineer prior to fissionable material processing.	1. Facility directive 29. 2. Training/postings.	C
2SX-PE13	MAT'L FORM: no precipitating agents	BFP installed on the line connecting the precipitation columns and the second pass evaporator. This prevents the backlog of oxalic acid into the SX operation.	1. Configuration control. 2. Annual surveill.	B

IROFS Identifier: cross-referenced with Preventive Controls in Table A-9. Parameters and Limits: describe actual parameter limits, and all attributes of the IROFS that are important to criticality safety. Management Measures: These are the measures needed to ensure IROFS availability and reliability. QA Grade: This is optional – all controls may be classified as Grade-A. If there is a graded QA Program, this signifies not the relative safety-significance of the control, but the degree of management attention needed once the item is installed to ensure its availability and reliability (*e.g.*, the siphon break is Grade-C, not because its failure is of minor NCS significance, but because once installed it requires essentially no maintenance.)

Note: Engineered features such as alarms and instrumentation needed to trigger an administrative response should be categorized as separate IROFS from the administrative controls; these design features are required to be maintained as IROFS.

6. DETERMINING MANAGEMENT MEASURES FOR SAFETY CONTROLS

Table A-8 is an acceptable way of listing those IROFS in all the accident sequences leading to consequences of concern. The IROFS listed should include all safety controls and all external events whose low likelihood is relied upon to meet the performance requirements of proposed 10 CFR 70.61. Staff reviews this list to determine whether measures have been applied to each safety control adequate to assure their continual availability and reliability in conformance to proposed 10 CFR 70.62(d). The types of management measures include maintenance, training, configuration management, audits and assessments, quality assurance, etc. These management measures are indicated in the Baseline Design Criteria (BDC) and described in greater detail in SRP Chapters 6.0 through 12.0 and 15.0. Safety controls meeting all the provisions of these chapters have acceptable management measures, that is, they comply with proposed §70.62(d). Safety controls may, with justification, have lesser management measures than those described. However, every item relied on for safety in accident sequences leading to consequence categories 2 or 3 should be assigned at least a minimal set of management measures. Specifically, in order to defend against common mode failure of all controls 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, (c) adequate labeling, training, or written procedures to assure the awareness of the operating staff of the safety function performed, (d) surveillance and corrective maintenance, and (e) preventive maintenance, if applicable.

If lesser or graded management measures are applied to some controls, Tables A-8 and A-9 and the narratives preceding them, in order to be acceptable, must identify to which 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 these measures, such as the surveillance interval, type of maintenance, or type of testing, be described as applied to each control. It is recognized that such specific measures must be applied differently to each control to whatever degree is necessary to achieve adequate reliability. It is the formality, documentation, and QA requirements applied to these

direct management measures that may be graded generically in a risk-informed manner.

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 risk index, and (2) the failure likelihood index, "T." In summary, items relied on to prevent or mitigate accidents with consequences in the two highest categories identified in proposed §70.61 should satisfy the applicable B.C. of proposed §70.64.

For each of the accident sequences evaluated in Table A-9 as being in an acceptable risk category (a risk index of less than or equal to 4):

(1) If the initiating event is not a control failure, then management measures for that event are not necessary. For sequences claimed to be highly unlikely or unlikely, the assessment that the initiating event has such a low frequency must be adequately justified in the application.

(2) Regardless of the degree to which this initiating event is relied on in the accident sequence, for accident sequences resulting in nuclear criticality, double contingency should still be established. This requires at least one more IROFS in the accident sequence, in addition to the initiating event, that requires management measures to ensure compliance with the double contingency principle.

(3) If the initiating event is a control failure, management measures for that IROFS should be applied sufficient to maintain the claimed failure frequency. The selection of management measures should take into consideration the failure likelihood assumed in finding the accident sequence risk acceptable, as well as the inherent nature of the control.

[Basis: If the required failure frequency index for a control with management measures applied (assumed in the accident sequence) is comparable to the failure index without management measures, such as for rigid dimensions of equipment not susceptible to changing, a relatively low level of management measures may be warranted.]

(4) If the initiating event is a control failure, management measures may be graded less than the highest level depending on the importance of the control to the overall risk of the accident sequence.

[Basis: If the unavailability of the IROFS makes a negligible increase in the overall risk, then that IROFS has a relatively low importance in the accident sequence. Assigning weights to the various IROFS in terms of management measures may be done by comparing the overall risk with and without (mitigated vs. unmitigated) that particular IROFS.]

7. RISK-INFORMED REVIEW OF SAFETY CONTROLS

The staff reviews the safety controls and external events listed in Table A-8 in a risk-informed manner as described in Section 5.5. The procedure for identifying systems of safety controls having higher risk significance is described in Section 5.5. These controls will be subject to a more detailed review by staff to assure their adequacy.

Table A-9: Example Accident Sequence Summary and Risk Index Assignment

Process: P^3 (Plutonium Purification Process) Node: 2SX (Second Pass Solvent Extraction)

Accident Sequence	Initiating Event (a)	Preventive Control 1 (b)	Preventive Control 2 (c)	Likelihood* Index T and Category C (d)	Conse-quence Category (e)	Risk Indices (f=d x e)	Comments & Recommendations
2SX-001	Pump chamber leaks	2SX-PE1: Pump chamber is safe volume F1 = -1. Regular maintenance prevents frequent pump failure. D1 = -3. Pump failure would be detected by oil presence in the solution in clear glass columns. Process continually monitored by operators.	2SX-AE1: Level switch keeps oil level at safe slab depth. Automatically actuates isolation valve and alarms if level exceeded. F2 = -2. Regular maintenance ensures low failure rate. D2 = -2. Biweekly surveillance.	T = -5 C = 1	3	3	
2SX-002	Heat exchanger tube leaks	2SX-AE2: Differential gauge alarms if pressure differential across evaporator not maintained. F1 = -1. Regular maintenance ensures low failure rate. D1 = -3. Failure would be detected during one shift because concentration monitored frequently for QA.	2SX-ADM1: Operator response required to respond to alarm if pressure differential lost. F2 = -2. Failure to evaporate would be noticed by operators on floor, and control room operator required by training and procedure to respond to alarm. Control room manned by two operators at all times. D2 = 0. Failure of this control may not be readily noted. Credit not taken.	T = -4 C = 2	3	6	This scenario requires other controls to ensure adequate low likelihood. Recommend installation of a drain line on the steam supply to prevent liquid accumulation.
2SX-003	Motive force causes potential backlog to nitric acid	2SX-PE2: Siphon break installed on supply line. F1 = -4. The most likely scenario is that the siphon break was never installed in the first place. There is a rigorous configuration control program for safety grade items. D1 = 0. All safety grade items audited annually to confirm their continued presence.	2SX-ADM2: Utility supply pressure not maintained above atmospheric. F2 = -2. Utilities used throughout facility for many different purposes. They are used frequently and so are tested on a continual basis. D2 = -2. Control room continually manned; these process variables are monitored constantly for QA purposes.	T = -5 C = 1	3	3	
2SX-004	Motive force causes potential backlog to DIW	2SX-PE3: Siphon break installed on supply line. see 2SX-003 for explanation.	2SX-ADM3: Utility supply pressure not maintained above atmospheric. see 2SX-003 for explanation.	T = -5 C = 1	3	3	

Accident Sequence	Initiating Event (a)	Preventive Control 1 (b)	Preventive Control 2 (c)	Likelihood* Index T and Category C (d)	Conse-quence Category (e)	Risk Indices (f=d x e)	Comments & Recommendations
2SX-005	Concentrated plutonium not stripped from organic	2SX-ADM4: Sufficient DIW added to ensure acid molarity low enough to guarantee stripping. Must be sampled and checked before stripping. 2SX-ADM5: Solvent regeneration columns M/Ss monitored weekly for uranium build-up. F1 = -2. Process variables (acid molarity and concentration) monitored shiftly and monitored continuously for QA purposes, ensuring their reliability D1 = -3. Major process upset would be noted by operators almost immediately.	2SX-PE4: BFP on organic buil chemical supply line. F2 = -2. Regular maintenance ensures low failure rate. D2 = -2. Failure would be detected during weekly surveillance.	T = -8 C = 1	3	3	
2SX-006	Solution spills from column	2SX-PE5: Columns are favorable geometry glass. F1 = -1. Columns have capacity to break even though they are sealed within a steel scaffold; operational history shows that this is an infrequent occurrence. D1 = -3. Breakage would be readily apparent. The process floor is continually manned and good housekeeping practices are instituted.	2SX-PE6: Catch pans are safe slab, and have sufficient area to hold the contents of more than two columns when filled to the maximum. F2 = -4. For this control to fail would either require improper installation, or the breakage of several columns. Configuration management reliability is judged to be -4. D2 = -3. See Control 1 explanation.	T = -7 C = 1	3	3	
...additional accident sequences would follow this...							
2SX-008	Earthquake occurs of sufficient strength to cause structural failure F = -5.	2SX-PE7: Columns separated at sufficient distance to ensure subcriticality. 2SX-PE5: Columns are favorable geometry. F1 = -3. If columns are subjected to extreme stresses they will tend to break rather than displace. Probability of displacing so that the columns would come to rest with their axes parallel is very low. D1 = -2. Several days is the longest that the condition would be likely to persist before control of the site was reestablished.	2SX-PE8: There are no water lines or other sources of water installed to burst in the event of an earthquake. F2 = -4. This is the standard frequency used elsewhere where a passive design feature that relies only on configuration management is used, when there are no other failure mechanisms. D2 = -2. The presence of water would be readily detected by responders following the earthquake.	T = -12 C = 1	3	3	This scenario takes credit for an external event. Site characteristics provide the likelihood of seismic activity and flood levels quoted.

*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 controls, hence the frequency is assigned under that control.

The final results column of Table A-9 gives the risk index for each accident sequence that was identified in the ISA. The risk index will be used by staff to identify all risk significant sets of controls. These sets of controls will be reviewed with greater scrutiny than controls established to prevent or mitigate accident sequences of low risk.

8. ACCIDENT SUMMARY AND RISK INDEX ASSIGNMENT FOR TABLE A-9

The definitions for the contents of each column in the accident summary tabulation, Table A-9, are provided below.

(1) Accident Sequence

This column is provided to list the accident sequences identified by the applicant in the ISA. It is important to the proper documentation of the ISA that the applicant subdivides the facility into a set of uniquely identified units, 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 Plutonium Purification process described in Section A6 has the unique identifying symbol P^3. The specific node corresponding to second pass solvent extraction has the unique identified 2SX. Additional identifier characters have been added to form the identifier, 2SX-001, to identify the first accident sequence identified in that node. Because the applicant should list all the facility safety 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 safety controls have been shown to prevent. By reviewing this table, the reviewer can then evaluate (1) the adequacy of the controls for preventing accidents and (2) the bases for making the consequence and likelihood assignments in the table.

(2) Initiating Event or Control Failure

This column is provided to list initiating events or control failures, typically identified in the process hazard analysis phase of the ISA, that may lead to consequences of concern. Initiating events are of several distinct types: (1) external events, such as hurricanes and earthquakes, (2) facility events external to the node being analyzed (e.g., fires, explosions, failures of other equipment, flooding from facility water sources), (3) deviations from normal of the process in the node (i.e., credible abnormal events), and (4) failures of safety controls of the node. The tabulated initiating events should only consist of those that involve an actual or threatened failure of safety controls, or that cause a demand requiring controls to function in order to prevent consequences of concern. The frequency index number for initiating events is referred to in the table using the symbol *"F."* Table A-4 provides criteria for assigning a value to *F*. Usually, insufficient room is present in a tabular presentation like Table A-9 to describe accurately the events indicated. Consequently, the applicant should provide supplementary narrative information to adequately describe each accident sequence of Table A-7. Cross referencing between this information and the table should be adequate; for

instance, the unique symbolic accident sequence identifiers can be used. Table A-7 is an example of a list of supplementary accident sequence descriptions corresponding to Table A-9.

(3) Preventive Control 1

This column is provided to list a control designed to prevent consequences of concern. If separate controls are used to prevent different consequences, separate rows in the table should be defined corresponding to each type of consequence. Sequences where two controls must simultaneously be in a failed state require assignment of three index numbers: the failure frequency of the first control, F_1, the duration of this failure, D_1, and the failure frequency of the second control, F_2. For such sequences, the initiating event is failure of the first control. In these cases, F_1 is assigned using Table A-4. The failure duration of the first control is assigned using Table A-6. Other sequences may be more easily described as a failure of the 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-5. The symbol "b" is used in the column heading for the indices associated with this control.

(4) Preventive Control 2

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

In cases where no second preventive control exists (especially when the B.C. require double contingency), this column should contain a description of the consequences resulting from the first control failure. For example, there are generally two ways to demonstrate double contingency – either by I) specifying a second independent control that has to fail concurrently before criticality is credible, or ii) showing by calculation that the worst credible physical conditions resulting from the control failure remain subclinical. References identifying the consequence calculations that relate to the accident sequences should be included somewhere in the table, such as in column "c" or "e."

(5) Likelihood Category

This column is provided to list the likelihood category number for the risk matrix, which is based on the total likelihood index for a sequence. The total likelihood index, T, is the sum of the indices for those events that comprise a sequence. These events normally consist of the initiating event, and failure of one or more controls, 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-3. The symbol "d" is used for this category number in the column heading.

(6) Consequence Category

This column is provided to assign the consequence category numbers 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 proposed 10 CFR 70.61. The symbol "e" is used for this category number in the column heading.

(7) 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 "f = d x e." Sequences with values of "f" less than or equal to "4" are acceptable. The risk index can be calculated as the product of the consequence category with the failure index of the first preventive control, giving a measure of the "unmitigated" risk, in the case where the second control is not available to perform its function. This is a way to assess the risk significance of the second control.

For sequences in which there is no second control specified, the unmitigated risk may be used to demonstrate an acceptable risk category. There may, however, be cases in which this is not possible; where there is a continuum of possible consequences resulting from occurrence of the accident sequence up to that point, credit may be taken for the unlikelihood of achieving an unacceptable physical state (*e.g.*, probability that the upset exceeds a subclinical mass). This will require a thorough, documented justification for the reviewer to find this approach acceptable.

(8) Comments and Recommendations

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

9. ALTERNATE METHODS OF PRESENTATION (FAULT TREES)

Table A-9 displays the results of the ISA Summary in a tabular format by accident sequence. This approach is commonly developed from a What-If hazard evaluation technique, which is but one of several methods available. The methods that may be used include What-If, HazOp, Failure Modes and Effects Analysis (FMEA), Fault

Figure A-2: Fault Tree for SX Operation

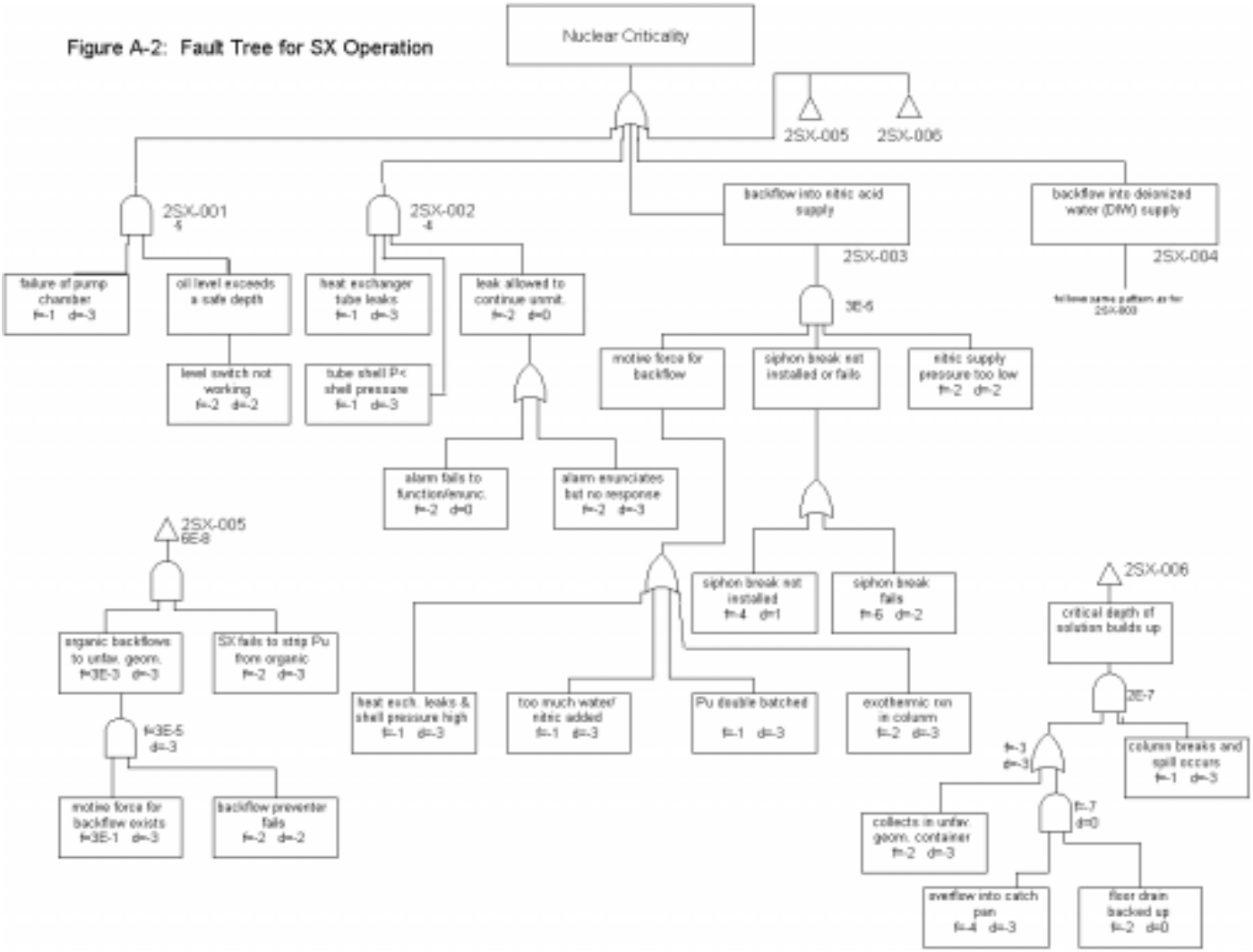
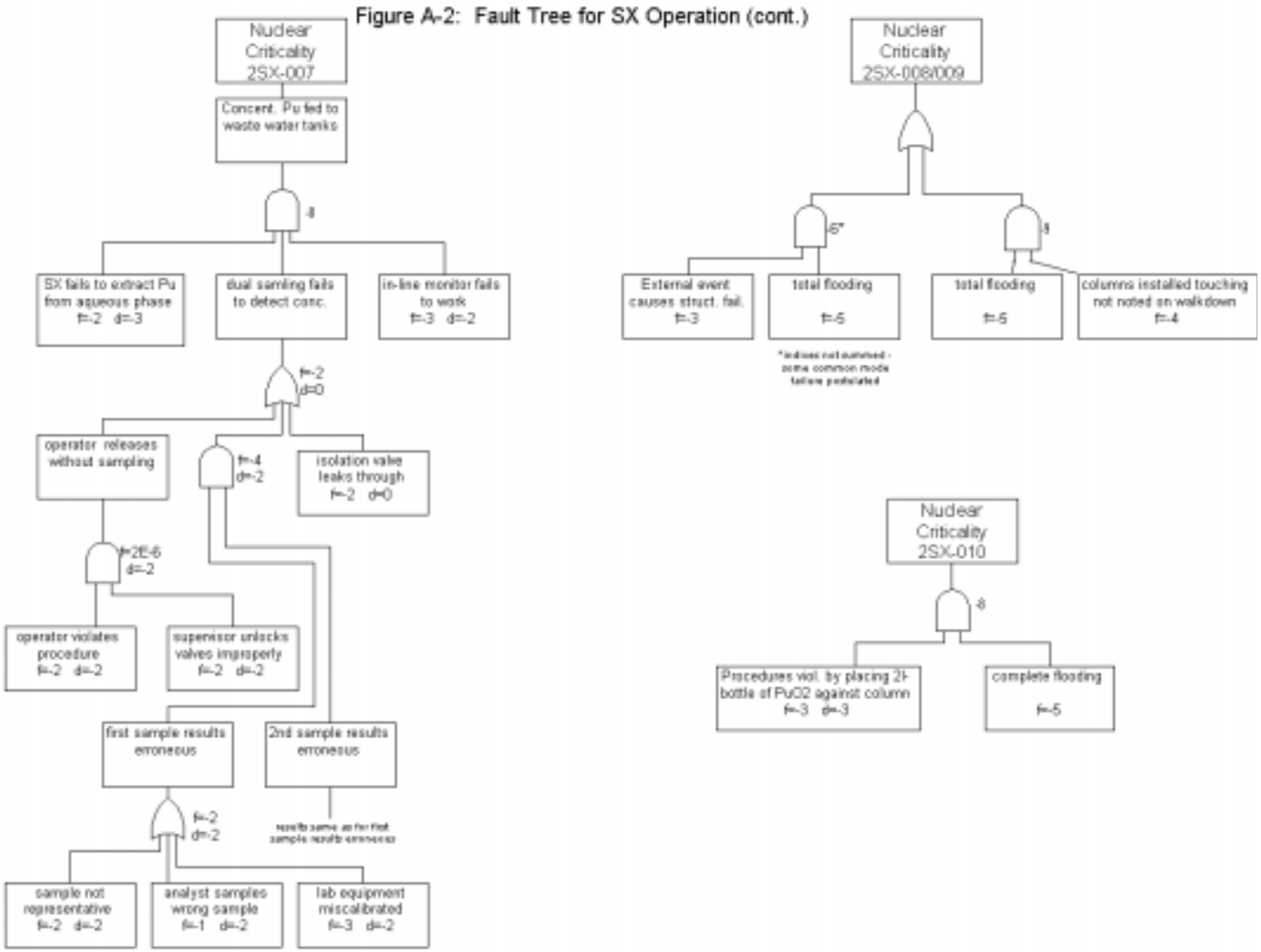


Figure A-2: Fault Tree for SX Operation (cont.)



Trees, and other methods. The What-If approach may be considered the least preferable of these approaches, particularly when there are a large number of accident sequences, as it is difficult to demonstrate completeness. That is, it will be difficult for the reviewer to verify that all credible accident sequences have been included in the hazard evaluation for a very complex process.

There are additionally reasons why a tabular format (Table A-9) may not be the best method of displaying the results of the ISA Summary for all processes. A variety of different techniques may be used rather than rigidly adhering to one format, if the multi-method approach enhances the clarity of the presented data. One of the main weaknesses of the tabular format is that it considers the accident sequence to consist of the failure of only two discrete controls. The establishment of double contingency may require more than two controls to ensure that at least two unlikely and concurrent upsets must occur before criticality is possible (and that the overall likelihood of criticality is highly unlikely). Several distinct controls may in general be combined into a single "control system." When grouped as shown in Figure A-2, there may be several distinct controls which must be grouped together to ensure each "leg" of double contingency is unlikely to fail. This definition of unlikely is in the context of the double contingency principle, which numerically is approximately $\leq 10^{-2}$, rather than the more restrictive value of $\leq 4 \times 10^{-4}$ as used in SRP Section 5.4.3.2(B)(ix). Use of this more conservative value would of course be acceptable, although it is highly doubtful whether many operations would be able to meet this without the virtual elimination of administrative criticality controls. Although this information may be presented in the table by listing multiple controls in each bin (*e.g.*, Scenarios 2SX-005 and -008), it would be more efficacious to use a fault tree (Figure A-2).

In addition, each accident sequence in the table considers the failure of the first control followed by failure of the second. Therefore there are actually two complementary accident sequences that must be considered in different rows of the table. This particular aspect of the logic – and the general logical flow of the accident as it unfolds–is masked by using an approach that follows a simple linear development of the sequence from initiating event to completion. In addition, the What-If approach often does not consider the control failure at a sufficiently high level. The answer to the question "*What if the pump chamber leaks into the oil reservoir*?" is often "*The pump cannot leak because....*" Considering the next to the top level event in the tree to be the loss of volume control ensures that the system will remain adequately subclinical even in the event that the pump failure occurs

The advantages of using a fault tree to present the ISA Summary data include: (1) the top-down approach of a fault tree (as opposed to the bottom-up approach of What-If) ensures that all credible changes in process conditions – or loss of controlled parameters–are considered; (2) robustness is ensured by considering the control failures at a sufficiently high level; and (3) the logical sequence of events that must occur to cause a criticality cannot be described thoroughly using the tabular approach. Figure A-2 shows a fault tree for the accident sequences that are described in Table A-9; a cursory review demonstrates that these diagrams present a much higher level of information than is contained in Table A-9. For example, in order to have a

criticality due to leakage through the heat exchanger into the steam supply, the following events would have occur: (1) the heat exchanger tubes would have to leak; and (2) the pressure on the tube side would have to drop below the pressure on the shell side; and (3) the leak would have to continue without being noticed, either by failure of the alarm to enunciate (mechanical) or failure of the operator to take appropriate actions (human error). This combination of events is then required to ensure that the overall consequence–getting concentrated uranium solution into the unfavorable geometry steam supply–is sufficiently unlikely (in fact, other controls are then recommended to reduce the likelihood index below -4). In addition, one can see that the loss of integrity of the evaporator tubes and loss of steam pressure are comparable events, and that reducing the frequency of mechanical failure of these items or the duration of alarm failure would result in the greatest drop in overall likelihood. In the event that other controls are credited in this scenario as a result of the recommendation, it would be difficult to convey the full amount of all the above information in the table.

A7. MIXED OXIDE BLENDING OPERATION

Oxide blending is a process whereby dry UO_2 and PuO_2 powder is combined to produce a homogeneous blend suitable for fabrication into mixed oxide fuel pellets and assemblies. The final mix consists of 20wt% PuO_2 (isotopically, ~96% ^{239}Pu and ~4wt% ^{240}Pu) and 80wt% U(0.7wt%)O_2. Process equipment downstream of the blending operation is designed with subclinical dimensions for 30wt% PuO_2 MOX. The main criticality controls in the blending operation are mass, moderation, and plutonium "enrichment" (defined for the purpose of this example as the weight percent of PuO_2 relative to the PuO_2-UO_2 blend).

A batch of UO_2 blendstock (~112 kg [246 lb]) is measured out into a favorable geometry feed hopper attached to a safety-grade scale. The material in the hopper is weighed and sampled for moisture, after which it is gravity fed into the favorable geometry blending hopper. This is a conical-bottom hopper which gravity drains into the cylindrical homogenizer. The low feed rate of the blendstock and plutonium oxide ensures that the powder attains a high degree of homogeneity as the two oxides are blended together. Homogeneity is not credited, however, for criticality safety until after the material passes through the homogenizer. In addition to ensuring criticality safety, moisture control is important to ensure that the powder will flow smoothly to ensure proper transfer and mixing.

PuO_2 powder is emptied from the 2-liter (0.45 gal) bottles into a plutonium oxide feed hopper through a hole in the bottom of a glovebox. This hopper is a 4-inch (10.2 cm) diameter cylindrical stainless steel vessel, which is heated to 150 °C (302 °F) to drive off residual moisture that may have accumulated. Several containers are emptied into the hopper until a mass of ~28 kg (61.6 lb) is reached. The powder is sampled and then gravity fed down a chute into the blending hopper. The flow rate of the plutonium oxide powder is controlled using a mass flow totalizer (MFT), which is interlocked to the plutonium feed valve; the feed rate is maintained at a slow rate using a stopcock on the input line. If the preset mass of plutonium oxide is exceeded, the MFT shuts the valve and prevents the overall plutonium "enrichment" in the blender from exceeding the safety limit

of 22wt% PuO_2. After blending, the material is agitated for 30 minutes before being sampled; only after two independent samples confirm the correct "enrichment" may the material be transferred to the cylindrical homogenizer for further processing. Following this, the *master mix* is ball-milled and sieved to ensure proper consistency before being combined with additional U(0.7wt%)O_2, which results in a *final mix* of ~4wt% Pu.

Table A-10 presents the main accident sequences in the oxide blending operation. Table A-11 shows the IROFS credited for double contingency during oxide blending. Table A-12 shows the main accident sequences and the preventive controls used.

A table of accident sequences is used to communicate the ISA Summary information for the oxide blending operation; this operation is a simpler process from a criticality safety standpoint than the solvent extraction. Since the double contingency logic is based on a relatively simple set of controls on moderation, mass, and plutonium isotonic, this system is much more amenable to a tabular approach. Fault trees could be used profitably for this system, but there is a much lower level of complexity than in the first example, and tables may be adequately used. Several tables will in general be needed to summarize the information that must be presented; these should be cross-referenced to allow clear traceability of the control logic. The contents of the tables and figure for the oxide blending process are summarized below:

1. PROCESS CRITICALITY FLOW DIAGRAM IN FIGURE A-3

   This process is inherently much simpler than the solvent extraction example considered above, from the standpoint of criticality safety. Note that in this case, the entire operation is conducted in favorable geometry equipment, so that there is no attempt to distinguish between favorable and unfavorable process steps graphically. One should note that labels have been attached to each piece of equipment relied on for safety, so that this diagram may be cross-referenced with the tables. Each component relied on for safety must be identified for incorporation into the configuration management program. For example, not only the mass flow totalizer, but also the interlock back to the PuO_2 supply valve, and the valve itself, must be controlled to ensure that the active feature that prevents too high a plutonium "enrichment" in the blend hopper remains available and reliable to perform its function.

2. ACCIDENT SEQUENCES IN Table A-10

   By displaying the accident sequences in the manner shown, it is immediately apparent that the criticality controls on the process are mass, moderation, and plutonium isotonic. Each of the accident sequences describes the initiating event and presents such information as the controls that prevent the loss of that controlled parameter, the safety significance of the initiating event, the probable cause, and so forth. The information should be succinctly provided in the ISA Summary to immediately put the accident sequences into the proper viewpoint.

3. ITEMS RELIED ON FOR DOUBLE CONTINGENCY IN TABLE A-11

Figure A-3 shows how a criticality flow diagram may be used effectively to summarize the contents of Table A-11. Please see Section A6 for a fuller discussion of this type of table.

4. SUMMARY OF ACCIDENT SCENARIOS AND RISK EVALUATION IN TABLE A-12

Note that Scenario MOB-001 has a consequence category of 0 (no consequences) instead of 3 (for criticality). This is not actually needed, because the likelihood index is sufficiently low based on the two preventive controls. However, this was done for illustrative purposes. As described in first entry in Table A-10, the loss of mass control due to the failure of both of these preventive controls cannot lead to criticality without a concurrent loss of moderation control. This should be documented in criticality calculations which would be referenced in the table. This is an acceptable way to treat accident scenarios where there is sufficient defense-in-depth that criticality cannot be achieved without the occurrence of additional events. In other words, the accident sequence defined by the failure of two preventive controls does not result in a criticality.

Scenarios MOB-006a and -006b (and MOB-010a and -010b) represent cases in which a single initiating event may occur due to two different causes. Generally deeper level events than the initiating event are not treated, but in this case it made sense to separate the sequences MOB-006 and -010 into more than one sub-sequence because different controls are needed for each pathway. Accident scenarios should be considered separate sequences if the controls relied on for safety are different, if the consequences are different (two scenarios leading to loss of mass control may result in different physical amounts and configurations), or likelihoods are different. Two accident sequences may have the same initiating events and the same consequences but different intermediate conditions or steps.

Figure A-3: Oxide Blending Operation

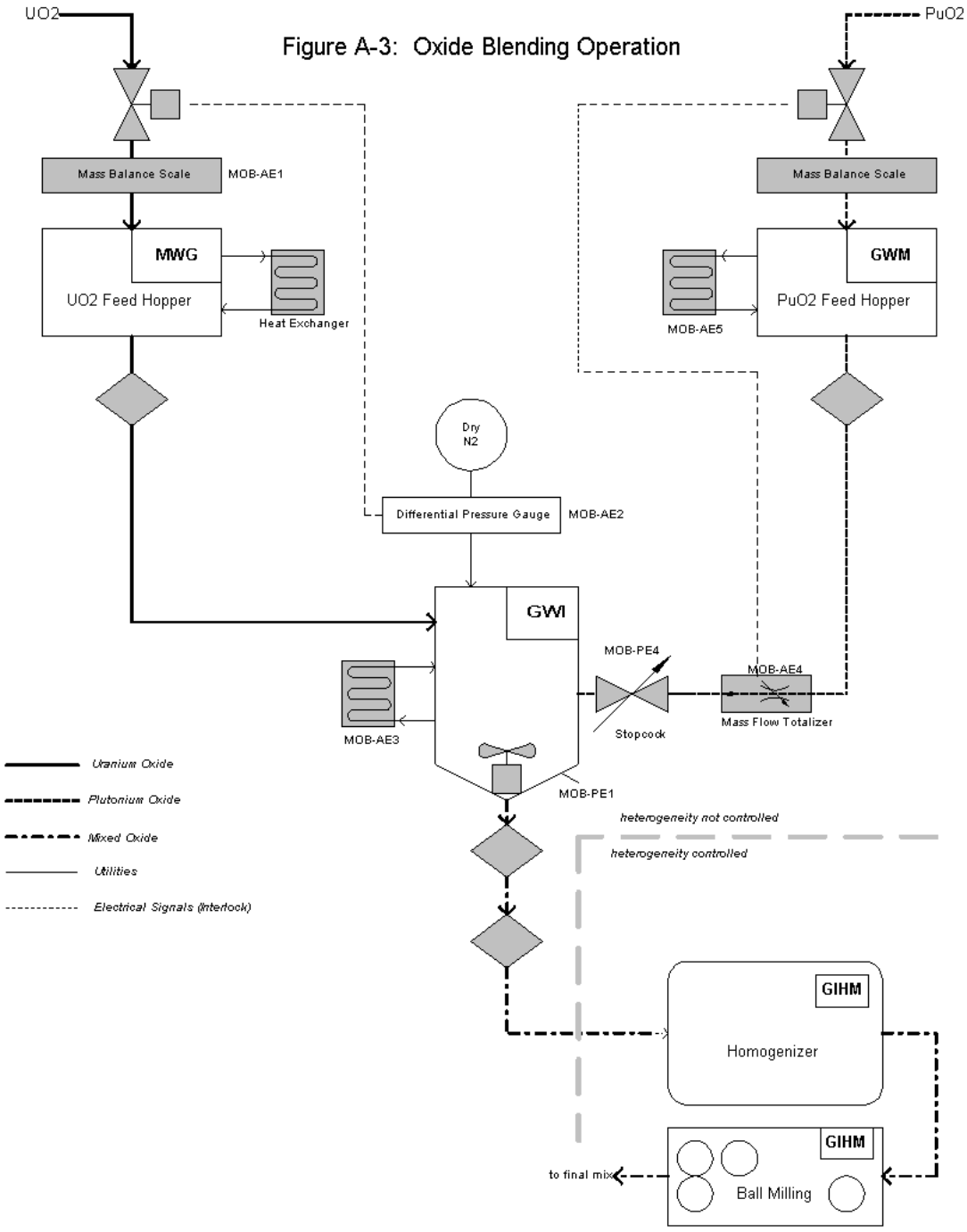


Table A-10: Accident Sequence Descriptions

Accident Sequence	DESCRIPTION
Loss of MASS	
MOB-001	The initiating event is exceeding the mass limit of the blend tank, by adding too much UO2 blendstock. This will have the effect of increasing the overall mass present, but will simultaneously decrease the plutonium "enrichment." The overall effect of this is to increase the distance from the subclinical curve of mass as a function of plutonium "enrichment" as more blendstock is added. The system is adequately subclinical under conditions of double batching uranium. To achieve criticality, this would have to be followed by a loss of moderation control.
MOB-002	The initiating event is exceeding the mass limit of the blend tank, by adding too much PuO2. This will have the effect of increasing both the overall mass and plutonium "enrichment." At ~33 kg PuO2 (72.6 lb) (and 23 wt%) the subclinical mass limit will be exceeded. Therefore, this could lead to criticality without any additional upsets and therefore dual controls are established on the plutonium mass.
MOB-003	The initiating event is exceeding the mass limit of the blend tank, by performing the blending operation while there is still blended oxide present from the previous batch in the tank. Assuming the previous batch was properly mixed, it would require an additional 50 kg (110 lb) of PuO2+UO2 to exceed the subclinical mass limit. Therefore this could lead to criticality without any additional upsets and therefore dual controls are established to ensure the blend tank is empty of material before another batch is started.
Loss of MODERATION	
MOB-004	The initiating event is exceeding the moderation limit (1 wt% H2O) by adding UO2 which has not been properly sampled. This could lead to criticality without any additional failures. Dual independent sampling is required to ensure moisture limits are adhered to. Also, material will not freely flow through orifice if wet.
MOB-005	The initiating event is exceeding the moderation limit (1 wt% H2O) by adding PuO2 which has not been properly sampled. This could lead to criticality without any additional failures. Dual independent sampling is required to ensure moisture limits are adhered to. Also, material will not freely flow through orifice if wet. In addition, both the plutonium feed hopper and blend hopper are heated. Material is added at a sufficiently slow rate that contact with the heated blendstock will cause moisture in the plutonium to be driven off.
MOB-006	The initiating event is exceeding the moderation limit (1 wt% H2O) by introduction of liquid water from overhead water lines or roof leaks. The blend tank is completely enclosed within an airtight and watertight enclosure. There are no overhead water lines allowed. The most likely cause of this scenario is backlog of condensate from the ventilation header, which serves to remove evolved water from the heated material. The ventilation header is sloped and equipped with drain lines to ensure against condensate backlog. Even in the event of water intrusion, the heating is sufficient to drive off any realistic accumulation of liquid water.
Loss of PLUTONIUM "ENRICHMENT"	
MOB-007	The initiating event is exceeding the plutonium "enrichment" by adding too little blendstock to the blending hopper. This will have the effect of increasing plutonium "enrichment" while decreasing the overall mass. This will eventually reach criticality without any additional failures, but only when more than half the original UO2 blendstock is omitted.
MOB-008	The initiating event is exceeding the plutonium "enrichment" by adding too much PuO2 feed to the blending hopper. This is identical to Scenario MOB-002 and will be discussed as a loss of mass control.
MOB-009	The initiating event is exceeding the plutonium "enrichment" by adding PuO2 to the blending hopper without first adding blendstock. This is the bounding case of Scenario MOB-007. Controls are established to ensure that blendstock is added and in the correct proportion before addition of PuO2 feed is allowed.
MOB-010	The initiating event is exceeding the plutonium "enrichment" by the formation of clumps of higher enrichment PuO2 in the blending hopper. This can be caused by I) too high a plutonium feed rate, ii) failure of the magnetic stirrer, iii) failure of the deflection plate, or iv) failure of moderation control, resulting in a more cohesive mix. Calculations show there are sufficient controls such that homogeneity is not necessary to ensure subcriticality. However, criticality could occur if this were followed by a loss of moderation control.

Table A-11: Criticality Safety Limits and Controls

IROFS Identifier	Parameters and Limits	IROFS Description	Management Measures	QA Grade
MOB-ADM1	MASS: UO_2 feed ~112 kg (246 lb)	Procedures, training, and postings require that the mass be checked and certified by an operator and supervisor prior to PuO_2 feed allowed.	1. Procedures and training. 2. Operator/supervisor must sign material balance sheets.	NA
MOB-AE1	MASS: UO_2 feed ~112 kg (246 lb)	Safety grade scale attached to feed hopper.	1. Weekly calibration using mass standards. 2. Tare weight re-certified whenever hopper is emptied.	A
MOB-PE1	MODERATION: Blend hopper is limited to 1wt% H_2O.	Blend tank comprises a welded stainless-steel barrier. Blending required to be under dry nitrogen atmosphere.		
MOB-AE2	MODERATION: Blend hopper is limited to 1wt% H_2O.	Blending required to be under a dry nitrogen atmosphere. IROFS is an differential pressure gauge interlocked to the feed supply valves and system alarm.	1. Monthly functional test. 2. Configuration control.	B
MOB-AE3	MODERATION: Blend hopper is limited to 1wt% H_2O.	Electric heater maintains powder at 150 °C (302 °F) in blend hopper. Low-T gauge and alarm interlocked to supply valves.	1. Weekly functional test. 2. Configuration control.	A
MOB-AE4	MASS: PuO_2 feed ~28 kg (61.6 lb)	Mass flow totalizer (MFT) interlocked to PuO_2 supply valve.	1. Configuration control. 2. Weekly function test.	A
MOB-PE2	GEOMETRY: diameter < 12.7 cm (5")	Diameter of oxide blender must be less than 12.7 cm (5").	Configuration control.	C
MOB-PE3	GEOMETRY: diameter < 10.2 cm (4")	Diameter of PuO_2 feed hopper must be less than10.2 cm (4").	Configuration control.	C
MOB-ADM2	MODERATION: Blend hopper is limited to 1 wt% H_2O	Procedures, postings, and training require the material in the UO_2 feed hopper to be sampled for moisture before it is released to the blending hopper. Supervisor concurrence required. Dual independent samples are required.	1. Procedures and training. 2. Lab QA procedures must be followed.	NA
MOB-AE5	MODERATION: Blend hopper is limited to 1 wt% H_2O	Electric heater maintains powder at 150 °C (302 °F) in PuO_2 feed hopper. Low-T gauge and alarm interlocked to supply valves.	1. Weekly functional test. 2. Configuration control.	A
MOB-ADM3	MODERATION: Blend hopper is limited to 1 wt% H_2O	Procedures, postings, and training require the material in the PuO_2 feed hopper to be sampled for moisture before it is released to the blending hopper. Supervisor concurrence required. Dual independent samples are required.	1. Procedures and training. 2. Lab QA procedures must be followed.	NA
MOB-ADM4	MASS: PuO_2 feed ~28 kg (61.6 lb)	Only a limited number of 2-liter (0.5 gal) bottles may be emptied into the PuO_2 feed hopper, such that the total mass does not exceed 28 kg (61.6 lb) as indicated on material balance sheets.	1. Procedures and training. 2. Material control program - the feed hopper is a process measurement node.	NA

IROFS Identifier	Parameters and Limits	IROFS Description	Management Measures	QA Grade
MOB-ADM5	MASS: Total blend hopper mass < 140 kg (308 lb)	Operators are required to check visually that the blend hopper is devoid of more than surface contamination after each campaign.	Procedures and training	NA
MOB-ADM6	MASS: Total blend hopper mass < 140 kg (308 lb)	Blend hopper must be NDA scanned after each campaign.	Procedures and training	NA
MOB-PE4	MODERATION: Blend hopper is limited to 1wt% H_2O.	Stopcock on PuO_2 feed line controls feed rate to 800 g/hr (1.8 lb/hr). This slow flow rate ensures that any moisture will be driven off on contact with the heated blendstock.	1. Flow rate checked during run by monitoring MFT. 2. Configuration control.	B
VEN-PE13	MODERATION: Blend hopper is limited to 1wt% H_2O.	Ventilation header must be sloped away from the blend hopper.	Configuration control.	C
VEN-PE15	MODERATION: Blend hopper is limited to 1wt% H_2O.	Ventilation header must be equipped with condensate drains at its lowest point, to prevent condensate backlog to the blend hopper.	1. Configuration control. 2. Periodic monitoring.	B
BLD16-65	MODERATION: Blend hopper is limited to 1wt% H_2O.	No overhead water lines are allowed in Building 16.	Configuration control.	C
MOB-ADM7	ISOTONIC: PuO_2 content 20wt%	Supervisor must check that UO_2 feed hopper is empty and that the appropriate mass has been added before PuO_2 transfer is authorized.	1. Procedures and training. 2. Material control program - the blendstock feed hopper is a process measurement node.	NA

Table A-12: Accident Sequence Summary and Risk Index Assignment

Accident Sequence	Initiating Event (a)	Preventive Control 1 (b)	Preventive Control 2 (c)	Likelihood* Index T and Category C (d)	Conse-quence Category (e)	Risk Indices (g=d x e)	Comments & Recommendations
MOB-001	Too much blendstock added.	MOB-ADM1: Blendstock mass certified before introduction of PuO_2. F1 = -3. Material control sensitivity ensures this receives appropriate attention and supervisor oversight. D1 = -2. Process is a batch process, campaign is running several days. Failure would be detected at start of subsequent campaign.	MOB-ADM7: Supervisor must ensure that the appropriate mass was emptied from blendstock feed hopper. F2 = -2. Required on checklist and reinforced by training and postings. D2 = -2. See MOB-001, Control 1.	T = -7 C = 1	0	0	Criticality not possible without an additional failure.
MOB-002	Too much PuO_2 added.	MOB-ADM4: No more than 28kg (61.6 lb) PuO_2 may be charged into the feed hopper. F1 = -3. Material control sensitivity ensures this receives appropriate attention and supervisor oversight. D1 = -2. See MOB-001, Control 1.	MOB-AE4: MFT limits total integrated PuO_2 which is transferred to blend hopper. F2 = -3. Regular maintenance and testing ensures reliability. D2 = -2. Functionally tested weekly.	T = -8 C = 1	3	3	
MOB-003	Mixed oxide not cleaned out before next batch started.	MOB-ADM5: Visual check that blend hopper empty before each campaign. F1 = -2. Required on checklist and reinforced by training and postings. D1 = -2. See MOB-001, Control 1.	MOB-ADM6: Blend hopper must be NDA scanned before each campaign. F2 = -2. Required on checklist and reinforced by training and postings. D2 = -2. See MOB-001, Control 1.	T = -5 C = 1	3	3	
MOB-004	Moderated blendstock added.	MOB-ADM2: Dual independent samples taken to confirm moisture level of blendstock. F1 = -3. Requires failure of two operators to follow procedures, and independence of sampling and lab analysis ensures reliability. D1 = -2. See MOB-001, Control 1.	MOB-AE3: Electric heater maintains temperature sufficient to drive off moisture in blend hopper. F2 =-4. Past history with this model of heater shows it to be very reliable. D2 = -2. Functionally tested weekly.	T = -8 C = 1	3	3	
MOB-005	Moderated PuO_2 added.	MOB-AE5: Electric heater maintains temperature sufficient to drive off moisture in feed hopper. F1 = -4. Past history with this model of heater shows it to be very reliable. D1 = -2. Functionally tested weekly.	MOB-AE3: Electric heater maintains temperature sufficient to drive of f moisture in blend hopper. F2 = -4. Past history with this model of heater shows it to be very reliable. D2 = -2. Functionally tested weekly.	T = -10 C = 1	3	3	

Accident Sequence	Initiating Event (a)	Preventive Control 1 (b)	Preventive Control 2 (c)	Likelihood* Index T and Category C (d)	Conse-quence Category (e)	Risk Indices (g=d x e)	Comments & Recommendations
MOB-006a	Water backlog from ventilation condensate.	VEN-PE13: Ventilation header sloped away from blend hopper. F1 = -3. The configuration control program requires installation according to design drawings and pre-startup verification. Several layers of management controls would have to fail to allow this to happen. D1 = 0. Would be checked during annual audit.	VEN-PE15: Ventilation header has condensate drains to prevent backlog. F2 = -3. The configuration control program requires installation according to design drawings and pre-startup verification. Several layers of management controls would have to fail to allow this to happen. D2 = 0. Would be checked during annual audit.	T = -6 C = 1	3	3	
MOB-006b	Water intrusion from external source.	MOB-PE1: Blend tank is watertight. F1 = -3. The ability of certified welders to ensure the integrity of welded vessels has been demonstrated. D1 = 0. Would be checked during annual audit.	MOB-AE2: Differential pressure gauge with interlock prevents introduction of feed if containment breached. F2 = -2. Based on past failure rate data when used in combination with HEPA filters. D2 = -1. Though sufficient to detect breach of the containment immediately (D ~ -5), its failure would be detected during monthly functional test. High demonstrated reliability means that D = -5 is actually more realistic.	T = -5 C = 1	3	3	
MOB-007	Too little blendstock added.	MOB-ADM1: Blendstock mass certified before introduction of PuO_2. F1 = -3. Material control sensitivity ensures this receives appropriate attention and supervisor oversight. D1 = -2. See MOB-001, Control 1.	MOB-ADM7: Supervisor must ensure that the appropriate mass was emptied from blendstock feed hopper. F2 = -2. Required on checklist and reinforced by training and postings. D2 = -2. See MOB-001, Control 1.	T = -7 C = 1	3	3	
MOB-008	same as MOB-002 (q.v.)						
MOB-009	PuO_2 added before blendstock.	MOB-ADM1: Blendstock mass certified before introduction of PuO_2. F1 = -3. Material control sensitivity ensures this receives appropriate attention and supervisor oversight. D1 = -2. See MOB-001, Control 1.	MOB-ADM7: Supervisor must ensure that the appropriate mass was emptied from blendstock feed hopper. F2 =-2. Required on checklist and reinforced by training and postings. D2 = -2. See MOB-001, Control 1.n	T = -7 C = 1	3	3	
MOB-010a	PuO_2 clump develops by: feed rate too high	MOB-PE4: Feed rate controlled by stopcock. F1 = -3. This is locked into place and tested before start-up. Has no moving or wear parts. D1 = -3. Failure would be detected during the course of one shift. Process is continually monitored by operators.		T = -6 C = 1	3	3	

Accident Sequence	Initiating Event (a)	Preventive Control 1 (b)	Preventive Control 2 (c)	Likelihood* Index T and Category C (d)	Conse-quence Category (e)	Risk Indices (g=d x e)	Comments & Recommendations
MOB-006a	Water backlog from ventilation condensate.	VEN-PE13: Ventilation header sloped away from blend hopper. F1 = -3. The configuration control program requires installation according to design drawings and pre-startup verification. Several layers of management controls would have to fail to allow this to happen. D1 = 0. Would be checked during annual audit.	VEN-PE15: Ventilation header has condensate drains to prevent backlog. F2 = -3. The configuration control program requires installation according to design drawings and pre-startup verification. Several layers of management controls would have to fail to allow this to happen. D2 = 0. Would be checked during annual audit.	T = -6 C = 1	3	3	
MOB-006b	Water intrusion from external source.	MOB-PE1: Blend tank is watertight. F1 = -3. The ability of certified welders to ensure the integrity of welded vessels has been demonstrated. D1 = 0. Would be checked during annual audit.	MOB-AE2: Differential pressure gauge with interlock prevents introduction of feed if containment breached. F2 = -2. Based on past failure rate data when used in combination with HEPA filters. D2 = -1. Though sufficient to detect breach of the containment immediately (D~-5), its failure would be detected during monthly functional test. High demonstrated reliability means that D = -5 is actually more realistic.	T = -5 C = 1	3	3	
MOB-007	Too little blendstock added.	MOB-ADM1: Blendstock mass certified before introduction of PuO_2. F1 = -3. Material control sensitivity ensures this receives appropriate attention and supervisor oversight. D1 = -2. See MOB-001, Control 1.	MOB-ADM7: Supervisor must ensure that the appropriate mass was emptied from blendstock feed hopper. F2 = -2. Required on checklist and reinforced by training and postings. D2 = -2. See MOB-001, Control 1.	T = -7 C = 1	3	3	
Accident Sequence	Initiating Event (a)	Preventive Control 1 (b)	Preventive Control 2 (c)	Likelihood* Index T and Category C (d)	Conse-quence Category (e)	Risk Indices (g=d x e)	Comments & Recommendations
MOB-010b	PuO_2 clump develops by: failure of moderation control	MOB-AE5: Electric heater maintains temperature sufficient to drive off moisture in feed hopper. F1 = -4. Past history with this model of heater shows it to be very reliable. D1 = -2. Functionally tested weekly.	MOB-PE4: Feed rate controlled by stopcock. F2 = -3. This is locked into place and tested before start-up. Has no moving or wear parts. D2 = -3. Failure would be detected during the course of one shift. Process is continually monitored by operators.	T = -9 C = 1	3	3	

*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 controls, hence the frequency is assigned under that control.