U.S. NUCLEAR REGULATORY COMMISSION
STANDARD REVIEW PLAN
OFFICE OF NUCLEAR MATERIAL SAFETY AND SAFEGUARDS

3.0 INTEGRATED SAFETY ANALYSIS

3.1 PURPOSE OF REVIEW

This chapter provides guidance for staff review of two types of information submitted by licensees or applicants:

1) Commitments regarding the applicant's Safety Program and Integrated Safety Analysis (ISA) pursuant to the requirements of 70.62.

2) ISA Summaries submitted in accordance with 10 CFR 70.62(c)(3)(ii) and 70.65.

In the case of license applications (either initial or for renewal), both types of information would be submitted. In the case of a license amendment, either or both types of information may be submitted, as needed to address the areas amended.

In the case of existing licensees, 10 CFR 70.62(c)(3)(i) requires a description of the ISA approach in a plan submitted by April 18, 2001. This SRP is not intended to explicitly address applicant submittal or NRC acceptance criteria for the 70.62(c)(3)(i) (ISA approach plan) requirement. That is because the rule requirement is of short duration (ending before publication of this SRP) and is applicable only to those entities licensed as of September 18, 2000. Separate guidance has been issued to affected licensees. However, a reasonable ISA approach plan will address many of the same descriptive elements regarding the ISA as would be described in a license application. Thus, an ISA approach plan meeting the acceptance criteria for the Safety Program and ISA commitments below would comply with section 70.62(c)(3)(i). The ISA Summary documenting completion of an ISA would be submitted later, in accordance with the approach and schedule in the plan.

Safety Program and ISA Commitments

The purpose for the review of commitments relative to the Safety Program and ISA, as presented in the license application, renewal, or amendment is to determine with reasonable assurance that the applicant will accomplish the requirements of Sec. 70.61, 70.62(a)(1), (2), and (3), 70.62(c)(1) and (2), 70.62(d), 70.64 for new facilities, and 70.72 for changes requiring an ISA.

ISA Results and Summary

All the information items needed to perform, or that are produced from, an ISA are referred to here as "ISA results." The ISA Summary is the principal document summarizing these results that is submitted to the NRC. The purpose of the review of the ISA Summary is to establish reasonable assurance that the applicant has performed the following tasks.

1. Conducted an ISA of appropriate detail for each applicable process, using methods and staff adequate to achieve the requirements of Sec. 70.62(c)(1) and (2).

2. Identified and evaluated in the ISA, all credible events (accident sequences) involving process deviations or other events internal to the plant (e.g., explosions, spills, and fires), and credible external events that could result in facility-induced consequences to the public, worker, or the environment, of the types specified in 10 CFR 70.61. External events normally include, as a minimum:
   1) natural phenomena events such as floods, high winds, tornados, and earthquakes;
   2) fires external to the facility;
   3) transportation accidents and accidents at nearby industrial facilities.

3. Designated engineered and administrative items relied on for safety (IROFS), and correctly evaluated the set of IROFS addressing each accident sequence, as providing reasonable assurance, through preventive or mitigative measures, that the safety performance requirements of 10 CFR 70.61 are met.

3.2 RESPONSIBILITY FOR REVIEW

Primary: Assigned staff licensing reviewer

Secondary: Technical specialists in specific areas

Supporting: Fuel Facility Inspection Staff

3.3 AREAS OF REVIEW

Two types of submittals are addressed by this chapter of the Standard Review Plan, (1) submittals containing descriptive commitments regarding the Safety Program and the ISA, and (2) ISA Summaries. The descriptive commitments regarding the Safety Program should be found in license applications, renewals, and amendments. ISA Summaries may be submitted for an entire existing facility, a new facility, a new process, or for altered processes requiring revision of the ISA.

The Safety Program and ISA commitments and descriptions to be reviewed consist of: 1) process safety information (70.62(b)), 2) methods used to perform the ISA, 3) qualifications of the team performing the ISA (70.62(c)(2)), 4) methods of documenting and implementing the results of the ISA, 5) procedures to maintain the ISA current when changes are made to the facility, and 6) management measures (70.62(d)). These commitments and descriptions, as appropriate, will be documented primarily within an ISA chapter, in the license application. However, commitments and descriptions regarding management measures will be in a separate chapter of an application, pursuant to Chapter 11 of this SRP.

The results of ISA analyses performed for compliance with the rule are presented in an ISA Summary. This ISA Summary may be submitted with an application for a new license, a license renewal, or a license amendment, but is not to be incorporated as part of the license.

The ISA Summary will be used to determine the adequacy of the applicant's ISA. The contents of the ISA Summary are specified in 10 CFR 70.65 and include, in addition to general facility information, descriptions of analyzed processes, descriptions of methods used to perform the

ISA, a description of the group of individuals performing the ISA, and descriptions of the IROFS that cause accident sequences to meet or exceed the performance requirements of 70.61.

The ISA and supporting documentation used in its preparation (e.g. piping and instrumentation drawings, engineered IROFS boundary descriptions, criticality safety analyses, dose calculations, process hazards analysis, process safety information, ISA worksheets) will be maintained at the facility site. The reviewer may need to consult the ISA and supporting documentation at the facility site to establish the completeness and acceptability of the ISA or, in the case of an existing facility, to visit the site to fully understand a process operation. For example, the reviewer should confirm that low-risk accident sequences not reported in the ISA Summary were correctly identified and analyzed in the ISA.

3.3.1 Safety Program and ISA Commitments

The staff reviews the application to determine whether the applicant's commitments to perform and maintain an ISA are adequate. In the following, the phrases, "process node" or "process", are used to refer to a single reasonably compact piece of equipment or workstation where a single unit process or processing step is conducted. A typical fuel cycle facility is divided into several major process lines or areas, each consisting of many process nodes. The areas of review for an ISA program are as follows:

1. The applicant's description of, and commitments to, a method for maintaining a current and accurate set of process safety information, including information on the hazardous materials, technology, and equipment used in each process. The applicant should explain this activity in detail in the description of its configuration management program (Section 11.1, "Configuration Management").

2. The applicant's description of, and commitments to, requirements for ISA team training and qualifications (Section 11.4, "Training and Qualification").

3. The applicant's description of, and commitments to, ISA methods, method selection criteria or specific methods to be used for particular classes of process nodes (usually process workstations). The review of the ISA methodology includes evaluating the applicant's methods in the following specific areas:

    a. Hazard identification.

    b. Process hazard analysis (accident identification).

    c. Accident sequence construction and evaluation.

    d. Consequence determination and comparability to 10 CFR 70.61.

    e. Likelihood categorization for determination of compliance with 10 CFR 70.61.

4. The applicant's description of, and commitments to, management procedures for conducting and maintaining the ISA. Specific review areas include the applicant's procedures for:
    (1) performance of, and updates to, the ISA;
    (2) review responsibility;
    (3) ISA documentation;

(4) reporting of ISA Summary changes per 10 CFR 70.72(d)(1) and (3), and
(5) maintenance of ISA records per 70.62(a)(2).

3.3.2 ISA Results

The staff reviews the ISA results (primarily the ISA Summary, but may include other ISA documentation) to find reasonable assurance that the applicant has performed a systematic evaluation of the hazards and credible accident sequences; and has identified IROFS and management measures that satisfy the performance requirements of 10 CFR 70.61. The review boundary includes those accidents that result in a release of radioactive material, a nuclear criticality event, or any other exposure to radiation resulting from use of licensed material. In addition, the staff reviews accidents involving hazardous chemicals produced from license materials. That is, chemicals that are licensed materials, or have licensed materials as precursor compounds, or substances that physically or chemically interact with licensed materials, and that are toxic, explosive, flammable, corrosive, or reactive to the extent that they endanger life or health. These include substances that are commingled with licensed material or are produced by a reaction with licensed material. If a chemical accident has the potential to cause, or reduce protection from, a radiation exposure accident, then it also must be addressed. On the other hand, event sequences having unmitigated consequences less than those identified in 10 CFR 70.61(c), once identified as such, do not require reporting in the ISA Summary.

The areas of review are as follows:

1. SITE: The site description in the ISA Summary (see Section 1.3, "Site Description") concerning those factors that could affect safety, such as geography, meteorology (e.g., high winds and flood potential), seismology, demography, and nearby industrial facilities and transportation routes.

2. FACILITY: The facility description in the ISA Summary concerning features that could affect potential accidents and their consequences. Examples of these features are facility location, facility design information, and the location and arrangement of buildings on the facility site.

3. PROCESSES: The description in the ISA Summary of each process analyzed as part of the ISA. Specific areas reviewed include basic process function and theory, functions of major components and their operation, process design and equipment, and process operating ranges and limits. It is expected that, for certain processes, additional information or a visit to the facility will be necessary to permit staff to understand the process.

4. TEAM QUALIFICATIONS: The applicant's ISA Team qualifications and ISA methods as described in the ISA Summary.

5. ISA METHODS: The description of ISA methods in the ISA Summary. If methods are adequately described in the license application, there will be no need to duplicate this information in the ISA Summary. Documentation of specific examples of the application of methods may be requested or reviewed on site to confirm understanding of specific methods.

6. CHEMICAL CONSEQUENCE STANDARDS: The applicant's quantitative standards for the chemical consequence levels specified in 10 CFR 70.61, as described in the ISA Summary.

7. LIKELIHOOD DEFINITIONS: The applicant's definitions of unlikely, highly unlikely, and credible used in §70.61 as described in the ISA Summary.

8. COMPLIANCE WITH 10 CFR 70.61: The information resulting from the ISA that demonstrates compliance with the performance criteria of 10 CFR 70.61. In addition to the information specifically required as noted in items 9 through 11 below, this information includes for each applicable process:

   a) The consequences evaluated for each postulated accident sequence; and comparison to the consequence levels identified in 10 CFR Part 70.61. Information, such as inventory, release path factors, supporting the results of the consequence evaluation.

   b) Information showing how each accident sequence has been assessed to have the likelihood required by 10 CFR 70.61.

   c) Information describing how each accident sequence, for each process, is protected sufficiently by the IROFS listed in the ISA Summary to comply with 10 CFR 70.61.

9. PROCESS HAZARDS: Information in the ISA Summary listing hazards and interactions for each process.

10. ACCIDENT SEQUENCES: Information provided in the ISA Summary that describes all accident sequences.

11. LIST OF IROFS: The list, in the ISA Summary, describing the IROFS for all accidents in each process sufficiently to understand their safety function in meeting the appropriate consequence and likelihood requirements of 10 CFR 70.61.

12. LIST OF SOLE IROFS: The list, in the ISA Summary, identifying those IROFS which are the sole item relied on in an accident sequence to assure compliance with 10 CFR 70.61.

13. CRITICALITY MONITORING: The information in the ISA Summary demonstrating compliance with the criticality monitoring requirements of 10 CFR 70.24.

14. NEW FACILITIES AND PROCESSES: The information in the ISA Summary demonstrating compliance with baseline design criteria required by 70.64(a)(1) through (5) and (7) through (10) for new facilities, or new processes at existing facilities, and required to be submitted in accordance with 10 CFR 70.65(b)(4). Since these elements all bear on the adequacy of IROFS, it is efficient to include their review in the ISA Summary review.

It is expected that, in addition to reviewing the application and ISA Summary, the NRC staff will select subsets of certain areas for which additional information will be reviewed, in some cases at the site. The method for selecting specific processes or accidents for additional review is described in Section 3.5 of this chapter, Review Procedures.

3.4 ACCEPTANCE CRITERIA

3.4.1 Regulatory Requirements

The requirement to perform an Integrated Safety Analysis (ISA) is specified in 10 CFR 70.62. 10 CFR 70.62(c) specifies requirements for the tasks comprising the ISA and the evaluation that credible high-consequence and intermediate-consequence events meet the safety performance requirements of 70.61. 10 CFR 70.72 sets forth requirements for keeping the ISA and its documentation current when changes are made to the site, structures, processes, systems, equipment, components, computer programs, and activities of personnel. 10 CFR 70.65(b) describes the contents of an ISA Summary.

The information to be included in the ISA Summary can be divided into four categories: (i) site and facility characteristics, (ii) ISA methodology, (iii) hazards and accident analysis, and (iv) items relied on for safety. The information requirements of each category, the corresponding regulatory citation and the section of NUREG-1520 Chapter 3 in which expectation for such information are presented below.

Information Requirements for the ISA Summary and Corresponding Part 70 and NUREG-1520 Citations

Information Category and Requirement	10 CFR 70 Regulatory Citation	NUREG-1520 Chapter 3 Reference
Site and Facility Characteristics:		
●site description	70.65(b)(1)	§3.4.3.2(2)(ii)
●facility description	70.65(b)(2)	§3.4.3.2(2)(I)
●compliance with baseline design criteria and ●criticality monitoring and alarms	70.64 (if applicable) & 70.65(b)(4)	§3.4.3.2(2)(viii) if applicable & §3.4.3.2(2)(ix)
ISA Methodology:		
●ISA methodology description	70.65(b)(5)	§3.4.3.2(2)(iii)
●ISA team description	70.65(b)(5)	§3.4.3.2(2)(iv)
●quantitative standards for acute chemical exposures	70.65(b)(7)	§3.4.3.2(2)(v)
●definition of unlikely, highly unlikely, and incredible	70.65(b)(9)	§3.4.3.2(2)(vi)
***Hazards and Accident Analysis*:**		
●description of processes analyzed	70.65(b)(3)	§3.4.3.2(3)(i)
●identification of hazards	70.65(b)(3)	§3.4.3.2(2)(vii)
●description of accident sequences	70.65(b)(3)	§3.4.3.2(3)(ii)
●characterization of high and intermediate-risk accident sequences	70.65(b)(3)	§3.4.3.2(3)(iii)
***Items Relied on For Safety*:**		
●list and description of items relied on for safety (IROFS)	§70.65(b)(6)	§3.4.3.2(4)(I)
●description of IROFS relation in analyzed accident sequences for assuring performance requirements	§70.65(b)(6)	§3.4.3.2(4)(I)
●IROFS management measures	§70.65(b)(4)	§3.4.3.2(4)(iii)
●list of sole IROFS	§70.65(b)(8)	§3.4.3.2(4)(ii)

3.4.2 Regulatory Guidance

Guidance applicable to performing an ISA and documenting the results is contained in NUREG-1513, "Integrated Safety Analysis Guidance Document." NUREG/CR-6410, “Nuclear Fuel Cycle Accident Analysis Handbook”, March 1998, provides guidance on acceptable methods for evaluating the chemical and radiological consequences of potential accidents.

3.4.3 Regulatory Acceptance Criteria

The acceptance criteria for an ISA are based on meeting the relevant requirements in 10 CFR Part 70, "Domestic Licensing of Special Nuclear Material." The ISA will form the basis for the safety program by identifying potential accidents, designating IROFS and management measures, and evaluating the likelihood and consequences of each accident sequence for

compliance with 10 CFR 70.61. Some of the acceptance criteria address the programmatic commitments made by the licensee to perform and maintain an ISA. The remainder of the criteria address the ISA results, as documented in the ISA Summary, and whether those documented results demonstrate that the applicant's IROFS and management measures can reasonably be expected to assure that the relevant accident sequences will meet the performance requirements of 10 CFR 70.61.

3.4.3.1 Safety Program and ISA Commitments

10 CFR Part 70 contains a number of specific safety program requirements related to the ISA. Acceptance criteria for those requirements addressed by contents of the ISA Summary appear in SRP section 3.4.3.2. These include the primary requirements that an ISA be conducted, and that it evaluate and show that the applicant's facility complies with the performance requirements of 10 CFR 70.61. Acceptance criteria for the other ISA requirements are provided in this section (3.4.3.1) of the SRP. For each required function there may be several necessary elements. These elements may include: organization, assignment of responsibilities, management policies, required activities, written procedures for activities, use of industry consensus standards, and technical safety practices. The applicant's commitment to each ISA requirement of the rule is acceptable if it:

a) describes each necessary ISA element sufficiently for the reviewer to understand how well it supports the safety program function;

b) commits to each ISA element as described, and to maintaining written procedures on site for carrying out that function, if necessary; and

c) provides reasonable assurance that the elements, as described, would be effective in accomplishing the ISA function.

In citing industry consensus standards, the applicant should delineate specific commitments in the standards which will be adopted. The applicant should provide justifications if a standard is not adopted in its entirety.

The staff will find the commitments in the application to ISA requirements acceptable, if the following criteria are met:

3. The applicant commits to compiling and maintaining an up-to-date database of process-safety information. Written process-safety information will be used in updating the ISA and in identifying and understanding the hazards associated with the processes. The compilation of written process-safety information shall include information pertaining to:

a. The hazards of all materials used or produced in the process. Information on chemical and physical properties such as toxicity, acute exposure limits, reactivity, and chemical and thermal stability such as are included on Material safety Data Sheets [meeting the requirements of 29 CFR 1910.1200(g)] should be provided.

b. Technology of the process. Information on the process technology should include a block flow diagram or simplified process flow diagram; a brief outline of the process chemistry; safe upper and lower limits for controlled parameters (e.g. temperature, pressure, flow, concentration); and evaluation of the health and safety consequences of process deviations.

c. Equipment used in the process. Information of a general nature on topics such as the materials of construction; piping and instrumentation (PI&Ds); ventilation; design codes and standards employed; material and energy balances; safety systems (e.g. interlocks, detection or suppression systems); electrical classification; and relief system design and design basis should be provided.

4. The applicant commits to keeping the ISA and ISA Summary accurate and up-to-date by means of a suitable configuration management system. The ISA must account for any changes made to the facility or its processes (e.g. changes to the site, operating procedures, control systems). Management policies, organizational responsibilities, revision time frame and procedures to perform and approve revisions to the ISA should be outlined succinctly. The applicant commits to evaluating any facility changes or changes in the process safety information that may alter the parameters of an accident sequence by means of the facility's ISA methodology. The applicant commits to using an ISA Team for any revisions to the ISA with member qualifications similar to those used in conducting the original ISA. The applicant commits to review of any facility changes that may increase the level of risk and, if dictated by revision of the ISA, to select and implement new or additional IROFS and appropriate management measures. The applicant commits to submitting to the NRC revisions of the ISA Summary within the time frame specified in 10 CFR 70.72(d)(3).

3. The applicant commits to promptly address any safety-significant vulnerabilities or unacceptable performance deficiencies identified in the ISA. The applicant commits to taking prompt and appropriate actions to address any vulnerabilities that are identified in an update of the ISA. If a proposed change results in a new type of accident sequence (e.g. different initiating event, significant changes in the consequences) or increases the risk of a previously analyzed accident sequence within the context of 10 CFR 70.61, the applicant commits to promptly evaluating the adequacy of existing IROFS and associated management measures and to making necessary changes, if required.

4. The applicant includes procedures and criteria for changing the ISA, along with its commitment to design and implement a facility change mechanism that meets the requirements of 10 CFR 70.72. The applicant should discuss the evaluation of the change within the ISA framework, and procedures and responsibilities for updating the facility ISA.

5. The applicant commits to engage personnel with appropriate experience and expertise in engineering and process operations to maintain the ISA. The ISA team for a process shall consist of individuals knowledgeable in the facility's ISA methodology and in the operation, hazards, and safety design criteria of the particular process.

6. 10 CFR 70.62(c) requires that an ISA of appropriate complexity be conducted for each process; and that it accomplish six (i-vi) results. The application is acceptable if it describes sufficiently specific methods and criteria that would be effective in accomplishing each of these tasks. Such effective methods and criteria are described in NUREG-1513, NUREG-6410, item 5 of SRP section 3.4.3.2, and Appendix A of this chapter. Sufficient features, criteria, equations, and data must be provided so that the staff can evaluate how the Integrated Safety Analyses of particular processes show that the performance requirements of 10 CFR 70.61 can be met.

7. The applicant commits to implement all IROFS (if not already implemented) and to maintain them so that they are available and reliable when needed. Management measures (which are evaluated using SRP Chapter 11) comprise the principal mechanism by which the reliability and availability of IROFS is assured.

3.4.3.2 ISA Results including ISA Summary

The preceding section addressed commitments to ISA requirements of the safety program. This section addresses whether the results of carrying out that program, i.e., the ISA methods and results, demonstrate compliance with the performance criteria of 10 CFR 70.61. Information in the ISA Summary should provide the basis for the staff's conclusions that there is reasonable assurance that the identified IROFS will satisfy the performance requirements of the rule. However, the basis for the staff conclusion would not be limited to a determination that the applicant's ISA program has the capability only to identify the appropriate IROFS. Rather, the focus of the staff review would be on the sufficiency of the IROFS identified in the ISA Summary. This requires a determination of whether the identified IROFS are adequate to control the potential accidents of concern at the facility. The accidents of concern are those whose consequences would be at the high and intermediate consequence levels absent any preventive or mitigative controls. In this context, adequacy means the capability of the IROFS to prevent the related accidents with sufficient reliability, or to sufficiently mitigate their consequences. This, in turn, requires staff to make a determination concerning the completeness of the accident sequences identified in the ISA Summary. To support such a review, the information in the ISA Summary needs to provide enough information concerning the accidents to which the IROFS relate to be able to assess their contributions to prevention or mitigation. The ISA Summary must contain enough information concerning the ISA procedures, methods, and human resources employed to have confidence that the potential accidents identified are reasonably complete.

The completeness and adequacy of the IROFS is not the only consideration for satisfying the performance requirements of 70.61. In addition, staff needs to determine that appropriate management measures will be in place that will ensure the availability and reliability of the identified IROFS, to the degree needed to satisfy the likelihood element of the performance requirement.

The following acceptance criteria address each of the content elements of the ISA Summary required by 10 CFR 70.65(b). For new facilities it is expected that the staff reviewing the ISA Summary will also evaluate those aspects of the design that address those baseline design criteria of 10 CFR 70.64 that apply to individual processes. Thus the content elements for which there are acceptance criteria include:

1) The site,
2) The facility,
3) The processes,
4) Team qualifications,
5) ISA methods,
6) Quantitative standards for chemical consequences,
7) Definitions of likelihood terms,
8) Information demonstrating compliance with the performance requirements,
9) Process hazards,
10) Description of accident sequences,
11) Descriptive list of all IROFS,
12) List of sole IROFS,
13) Information demonstrating compliance with the requirements for criticality monitoring,
14) Information demonstrating compliance with the requirements for new facilities.

The acceptance criteria that follow are guidance to the reviewer in determining whether the contents of the above elements are sufficient to provide reasonable assurance that the applicant's process-safety design and safety procedures meet the performance requirements of 10 CFR 70.61 and other requirements of 10 CFR Part 70.

1. SITE

The description in the ISA Summary of the site for processing nuclear material is considered acceptable if the applicant includes, or references, the following safety-related information with emphasis on those factors that could affect safety:

a. A description of the site geography, including its location from prominent natural and man-made features such as mountains, rivers, airports, population centers, possibly hazardous commercial and manufacturing facilities, transportation routes, etc., adequate to permit evaluation of: i) the likelihoods of accidents caused by external factors; and ii) the consequences of potential accidents.

b. Population information, based on recent census data, that shows population distribution as a function of distance from the facility adequate to permit evaluation of regulatory requirements, including exposure of the public to consequences listed in 10 CFR 70.61.

c. Characterization of natural phenomena (e.g., tornadoes, hurricanes, floods, and earthquakes) and other external events sufficient to assess their impact on plant safety and to assess their likelihood of occurrence. At least the 100 year flood should be postulated, consistent with U.S. Army corps of Engineers flood plain maps. Also, an earthquake acceleration on the site associated with an earthquake of 10^{-3}/yr likelihood on the nearest capable fault should be evaluated for new facilities and processes, to determine its resulting consequences on the structural integrity of the facility. A higher likelihood may be justified on the basis of relatively low hazards and/or short remaining facility or process lifetime. The discussion identifies all design basis natural events for the facility, indicates which events are considered incredible, and describes the basis for that determination. The assessment also indicates which events could occur without adversely impacting safety.

2. FACILITY

The description of the facility is considered acceptable if the applicant identifies and describes the general features that affect the reliability or availability of items relied on for safety. If such information is available elsewhere in the application, reference to the appropriate sections is considered acceptable. The information provided should adequately support an overall understanding of the facility structure and its general arrangement as it pertains to the ISA. As a minimum, the applicant adequately identifies and describes:

a. The facility location and the distance from the site boundary in all directions, including the distance to the nearest resident and distance to boundaries in the prevailing wind directions.

b. Design information regarding the resistance of the facility to failures caused by credible external events, when those failures may produce consequences exceeding those identified in 10 CFR 70.61.

c. The location and arrangement of buildings on the facility site.

3. PROCESSES

The description of the processes analyzed as part of the ISA [70.62(c)(1) (i-vi)] is considered acceptable if it describes the following features in sufficient detail to permit an understanding of the theory of operation, and to determine compliance with the performance requirements of the rule. A description at a systems level is acceptable provided it permits the staff to conduct adequately: 1) an evaluation of the completeness of the hazard and accident identification tasks, and 2) an evaluation of the likelihood and consequences of the accidents identified. If the information is available elsewhere in the application and is adequate to support the ISA, reference to the appropriate sections is considered acceptable. The information provides an adequate explanation of how the IROFS reliably prevent the process from exceeding safety limits for each case identified in the ISA results where they are needed.

a. Basic process function and theory. This information includes a general discussion of the basic theory of the process.

b. Major components–their function and operation. This information includes the general arrangement, function, and operation of major components in the process. It includes arrangement drawings and process schematics showing the major components and instrumentation and, if appropriate, chemical flow sheets showing compositions of the various process streams.

c. Process design and equipment. This information includes a discussion of process design, equipment, and instrumentation that is sufficiently detailed to permit an adequate understanding of the results of the ISA. It includes schematics indicating safety interrelationships of parts of the process. In particular, it is usually necessary for criticality safety to diagram the location and geometry of the fissile and other materials in the process, for both normal and bounding abnormal conditions. This can be done using either schematic drawings or textual descriptions indicating the location and geometry of fissile materials, moderators, etc. sufficient to permit an understanding of how the IROFS limit the mass, geometry, moderation, reflection, etc..

d. Process operating ranges and limits. This information includes the operating ranges and limits for measured process variables (e.g., temperatures, pressures, flows, and compositions) that are controlled by IROFS to ensure safe operation of the process. The process operating limits and ranges are considered acceptable if they are consistent with those evaluated as adequate for safety in the ISA. One acceptable way of presenting this information is as a tabular summary of all IROFS grouped according to hazard type (i.e. nuclear criticality, radiological hazards, chemical hazards, etc.) as shown in Appendix A, Table A-12.

4. TEAM QUALIFICATIONS

The ISA teams [70.62(c)(2)] and their qualifications as stated in the ISA Summary are acceptable if the following criteria are met:

a. The ISA team has a team leader who is formally trained and knowledgeable in the ISA methodology chosen for the hazard and accident evaluations. In addition, the team leader should have an adequate understanding of all process operations and hazards under evaluation, but should not be the responsible, cognizant engineer or expert for that process.

b. At least one member of the ISA team has thorough, specific, and detailed experience in the process under evaluation.

c. The team represents a variety of process design and safety experience in those particular safety disciplines relevant to hazards that could credibly be present in the process including, if applicable, radiation safety, nuclear criticality safety, fire protection, and chemical safety disciplines.

d. A manager provides overall administrative and technical direction for the ISA.

5. ISA METHODS

It is important that the reviewer determine the methods and criteria used in the ISA , and whether they are adequate in principle, before evaluating results for individual processes. The summary of ISA methods is considered acceptable if it describes the methods used for each ISA task. In accordance with NUREG-1513, it is expected that different specific analytical techniques will be used in different processes depending on their nature and complexity. Specific acceptance criteria for methods used in each ISA task are as follows:

a. Hazard Identification Method. The hazard identification method selected is considered acceptable if it:

i. Provides a list of materials (radioactive, fissile, flammable, and toxic) and conditions that could result in hazardous situations (e.g., loss of containment of licensed nuclear material). The list includes maximum intended inventory amounts and the location of the hazardous materials at the facility.[1]

ii. Determines potential interactions between materials or conditions that could result in hazardous situations.

b. Process Hazard Analysis Method. The method for performing process hazard analysis is acceptable if it consists of selecting one of the individual methods described in NUREG-1513 in accordance with the selection criteria of that document. Individual methods not described in NUREG-1513 may be acceptable provided that:

i. Criteria are provided for their use for an individual process that are consistent with the principles of the selection criteria in NUREG-1513.

ii. It adequately addresses all the hazards identified in the hazard identification task. If an identified hazard is eliminated from further consideration, such action is justified.

iii. It provides reasonable assurance that the applicant can identify all significant accident sequences (including the IROFS used to prevent or mitigate the accidents) that could result in the consequences identified in 10 CFR 70.61[2].

[1] At a minimum, the following hazardous materials should be included in the inventory list if present on-site: ammonia, fines (UO_2 dust, beryllium), flammable liquids and gases, fluorine, hydrofluoric acid, hydrogen, nitric acid, organic solvents, propane, uranium hexafluoride, and Zircalloy.

[2] The release of hazardous chemicals is of regulatory concern to NRC only to the extent that such hazardous releases result from the processing of licensed nuclear material or have the potential for adversely affecting radiological safety.

iv. It takes into account the interactions of identified hazards and proposed IROFS, including system interactions, to ensure that the overall level of risk at the facility is consistent with the requirements of 10 CFR 70.61.

v. It addresses all modes of operation including startup, normal operation, shutdown, and maintenance.

vi. It addresses hazards resulting from process deviations (e.g., high temperature, high pressure); initiating events internal to the facility (e.g., fires or explosions); and hazardous credible external events (e.g., floods, high winds, and earthquakes, airplane crashes). The applicant provides justification for determinations that certain events are not credible and, therefore, not subject to the likelihood requirements of 10 CFR 70.61.

vii. It adequately considers initiation of, or contribution, to accident sequences by human error through the use of human-systems interface analysis or other appropriate methods.

viii. It adequately considers common mode failures and system interactions in evaluating systems that are to be protected by double contingency.

ix. The ISA Summary provides justification that the individual method would effectively accomplish ii through viii above.

e. Consequence Analysis Method. The methods used for ISA consequence evaluation, as described in the ISA Summary are acceptable if:

i. They are consistent with the approaches described in the Nuclear Fuel Cycle Facility Accident Analysis Handbook (NUREG/CR-6410, March 1998); and

ii. They are scientifically correct as a reasonable estimate; and

iii. Their use of generic assumptions and data is reasonably conservative for the types of accidents analyzed.

d. Likelihood Evaluation Method. The method for evaluation of the likelihood of accident sequences, as described in the ISA Summary, is considered acceptable if it meets the criteria described below such that, given the IROFS and management measures described by the applicant, the staff analyst can find reasonable assurance that the performance criteria of 70.61 are met. Specific criteria are:

i. The method clearly shows how each IROFS involved acts to prevent or mitigate the accident sequence being evaluated.

ii. When multiple IROFS are involved in an accident sequence, the method considers the interaction of all the IROFS involved, as in a logic diagram or tabulation, that accounts for the impact of redundancy, independence, and surveillance to correct failures on the likelihood of occurrence of the accident.

iii. The method has objective criteria for evaluating, at least qualitatively, the likelihood of failure of individual IROFS. Such likelihood criteria should include the following when applicable: means to limit potential failure modes, the magnitude of safety

margins, the type of engineered equipment (active or passive) or human action that constitutes the IROFS, and the types and grading, if any, of the management measures applied to the IROFS.

iv. Finally, the method evaluates each accident sequence as unlikely, highly unlikely, or neither, as defined by the applicant in accordance with subsection 3.4.3.2, Item 7 of this chapter.

v. For nuclear criticality accident sequences, the method evaluates compliance with 70.61(d). That is, even in a facility with engineered featuresto limit the consequences of nuclear criticalities, preventive control(s) must be in place that are sufficient to assure that the likelihood of criticality is controlled to be "unlikely." A moderately higher standard of likelihood may be permitted in preventing such events consistent with ANSI/ANS Standard 8.10. In particular, criticality cannot result from any single IROFS failure. In addition, potential criticality accidents must meet an approved margin of subcriticality for safety. Acceptance criteria for such margins are reviewed as programmatic commitments, but the ISA methods and Summary must consider and document the actual magnitude of those margins when they are part of the reason why the postulated accident sequence resulting in criticality is unlikely.

One acceptable method of likelihood evaluation is described in Appendix A.

6. QUANTITATIVE STANDARDS FOR CHEMICAL CONSEQUENCES.

The applicant's description of proposed quantitative standards used to assess consequences from acute chemical exposure to licensed material or chemicals produced from licensed material is acceptable if:

a. There are unambiguous quantitative standards for each of the applicable hazardous chemicals on site corresponding to, and consistent with, the qualitative standards each of the following sections of 10 CFR: 70.61(b)(4)(i), 70.61(b)(4)(ii), 70.61(c)(4)(i), and 70.61(c)(4)(ii).

b. The quantitative standard of §70.61(b)(4)(i) proposed for chemical consequences correctly categorizes as such, all exposures that could endanger the life of a worker. The applicant is appropriately conservative in applying the language "could endanger" so as to include exposures that would result in death, consistent with the methods used for EPA Acute Exposure Guidelines.

c. The quantitative standards for 70.61(b)(4)(ii) and 70.61(c)(4)(i) will correctly categorize as such, all exposures that could lead to irreversible or other serious, long-lasting health effects to individuals. As with b. above, the standard selected should have appropriate conservatism.

d. The quantitative standard for 70.61(c)(4)(ii) will correctly categorize as such, all exposures that could cause mild transient health effects to an individual.

As indicated in the Consequence Severity Category Table of Appendix A (Table A-1), the staff finds the use of the ERPG and AEGL series of standards to be acceptable sets, each meeting the performance criteria of 10 CFR 70.61. However, since such standards may not cover all the appropriate chemicals, the ISA Summary to be acceptable must list the actual values selected for each chemical, and provide information or a reference justifying that they meet the

acceptance criteria stated above. When the chemical is covered by ERPG or AEGL values, a reference to this fact is sufficient.

7. DEFINITIONS OF LIKELIHOOD TERMS

10 CFR 70.65 requires that the applicant's ISA Summary provide definitions of the terms unlikely, highly unlikely, and credible. The applicant's definitions of these terms are acceptable if, when used with the applicant's method of assessing likelihoods, they provide reasonable assurance that the performance requirements of 10 CFR 70.61 can be met. The applicant's method of likelihood evaluation and the definitions of the likelihood terms are closely related. Qualitative methods require qualitative definitions. Such a qualitative definition would identify the qualities of IROFS controlling an accident sequence that would qualify that sequence as "unlikely" or "highly unlikely".

An applicant may use quantitative methods and definitions for evaluating compliance with 10 CFR 70.61, but nothing in this SRP should be construed as an interpretation that such methods are required. In fact, it is recommended that, in any case, the reviewer focus on objective qualities and information provided concerning accident likelihoods.

Section 70.61 requires that credible high-consequence events be highly unlikely. Thus the meaning of the phrase "highly unlikely" is on a per event basis. The same is true for the terms "unlikely" and "credible." Hence, applicant definitions should be on a per event basis. The events referred to are occurrences of consequences, which is herein synonymous with the phrase "accident sequence". This is important to recognize since there may be hundreds of potential accident sequences identified in an ISA. Thus the likelihood of each individual sequence must be quite low.

ACCEPTANCE CRITERIA FOR THE DEFINITION OF "CREDIBLE"

10 CFR 70.65 requires that the applicant define the term "credible". This term "credible" is used in 10 CFR 70.61 to state the performance requirements that all credible events be controlled to be unlikely or highly unlikely, as appropriate. If an event is not credible, then controls are not required to prevent or mitigate the event. Thus, to be 'not credible' could be used as a criterion for exemption from use of controls. There is a danger of circular reasoning here. In the safety program embodied in the rule, the fact that an event is 'not credible' must not depend on any plant feature that could credibly fail to function, or be rendered ineffective as a result of a change to the system. Each plant feature that is needed to assure that accident events are sufficiently unlikely is an "item relied on for safety" (IROFS). There must be high assurance, provided by management measures, that such features are not removed or rendered ineffective during system changes. One cannot claim that a process does not need IROFS because it is 'not credible' due to characteristics provided by IROFS.

Three independent acceptable sets of qualities, any one of which could define an event as not credible, are:

1) An external event whose frequency of occurrence can conservatively be estimated as less than once in a million years.

2) A process deviation that consists of a sequence of many unlikely human actions or errors for which there is no reason or motive. In determining that there is no reason for such actions, consideration must have been given to a wide range of possible motives, short of intent to

cause harm. Necessarily, no such sequence of events can ever have actually happened in any fuel cycle facility.

3) Process deviations for which there is a convincing argument, based on physical laws, that they are not possible, or are unquestionably extremely unlikely. The validity of the argument must not be dependent on any feature of the design or materials which is controlled by the plant's system of IROFS or management measures.

The implication of the use of "credible" in 10 CFR 70.61 is that events which are not "credible" may be neglected. For this to be acceptable on a risk basis, unless the event is impossible, it must be of negligible likelihood. Negligible likelihood means sufficiently low that, considering the consequences, the addition to total risk is small. Note that consideration must thus be given to how many such events have, in fact, been neglected. An applicant may demonstrate, by quantitative reasoning, that a particular event is of negligible frequency. Such a demonstration must be convincing despite the absence of designated IROFS. Typically, this can only be achieved for external events known to be extremely unlikely.

ACCEPTANCE CRITERIA FOR QUALITATIVE DEFINITIONS OF LIKELIHOOD

If the applicant's definitions are qualitative, they are acceptable if that they are:

a) reasonably clear and based on objective criteria, and

b) can reasonably be expected to consistently distinguish accidents that are highly unlikely from those that are merely unlikely.

By the phrase "objective criteria" is meant the extent to which the method relies on specific identifiable characteristics of a process design, rather than subjective judgements of adequacy. Objective criteria are needed to achieve consistency. By consistency is meant the degree to which the same results are obtained when the method is applied by different analysts. This is important in order to maintain an adequate standard of safety because ISAs of future plant modifications may be performed by individuals not involved in the initial ISA.

Reliability and Availability Qualities

Qualitative methods of evaluating the likelihood of an accident sequence involve identifying the reliability and availability qualities of each of the events that constitute the sequence. The following lists of qualities is not necessarily complete, but contains many of the factors most commonly encountered. Some of these qualities relate to the characteristics of individual IROFS, such as:

1) safety margin in the controlled parameter compared to process variation and uncertainty,
2) whether the IROFS is an active engineered control, a passive engineered control, an administrative control, or an enhanced administrative control,
3) the type and grade of management measures applied to the control,
4) fail-safe, self-announcing, or surveillance measures to limit down time.
5) failure modes
6) demand rate
7) failure rate

Other reliability qualities relate characteristics of the system of IROFS protecting against the accident sequence as a whole, such as:

8) defense-in-depth,
9) degree of redundancy,
10) degree of independence,
11) diversity,
12) vulnerability to common cause failure.

Methods of likelihood evaluation, and the definitions of the rule's likelihood terms, may mix qualitative and quantitative information. Certain types of objective quantitative information may be available concerning specific processes in a plant. Some examples of such objective quantitative information are:

1) reports of failure modes of equipment or violations of procedures recorded in maintenance records or corrective actions programs,
2) the time intervals at which surveillance is conducted to detect failed conditions,
3) the time intervals at which functional tests or configuration audits are held,
4) for a fail-safe, monitored, or self-announcing IROFS, the time it takes to render the system safe;
5) demand rates, that is, how frequent are the demands on an IROFS to perform. Some situations amount to effectively continuous demand.

Such items of quantitative information should be considered in evaluating the likelihood of accident sequences, even in purely qualitative evaluations. For example, knowing the value to which down time is limited by surveillance can indicate that a system's availability is extremely high. For redundant systems, such high availability can virtually preclude concurrent independent failures of the multiple controls.

Acceptance Criteria for Likelihood Indexing Methods

One acceptable type of definition for the likelihood terms "unlikely" and "highly unlikely" could be based on a risk indexing method. Such a method is described in the example in Appendix A. The example described in Appendix A is intended to rely primarily on a qualitative evaluation of reliability / availability factors. In such methods, qualitative characteristics of the system of IROFS, such as those listed above, are used to estimate a quantitative likelihood index for each accident sequence. The definition of "unlikely" then is an acceptable limit on this likelihood index.

Acceptance Criteria for Purely Qualitative Methods

A purely qualitative method of defining "unlikely" and "highly unlikely" is acceptable if it incorporates all of the applicable reliability and availability qualities to an appropriate degree. For example, one statement of applicable qualities is double contingency protection:

Double Contingency Protection: The quality of a process design that incorporates sufficient factors of safety to require at least two unlikely, independent, and concurrent changes in process conditions before a criticality accident is possible.

Double contingency addresses explicitly several reliability / availability qualities; namely:

factors of safety: safety margins

at least two:	redundancy
unlikely:	low failure rate, low down time of one of two controls
concurrent:	low down time
independent:	independence
process conditions:	physical events, not virtual human errors

One acceptable definition of highly unlikely is a system of IROFS that possesses double contingency protection where each of the applicable qualities is present to an appropriate degree. For example, as implied by the modifier, “at least”, sometimes more than just two-fold redundancy may be appropriate.

A qualitative method may also be proposed for defining “unlikely” Such a qualitative method might simply list various combinations of reliability qualities for a system of IROFS that would qualify as “unlikely”. For example, a single high reliability IROFS, such as an engineered hardware control with a high grade of applicable management measures might qualify to be considered “unlikely to fail.” Systems relying on administrative controls would normally have to make use of enhancing qualities such as large safety margins and redundancy in order to qualify as “unlikely to fail”. A single simple administrative control, regularly challenged, without any special safety margin or enhancement, where a single simple error would lead to an accident, would not qualify as “unlikely” to fail.

ACCEPTANCE CRITERIA FOR QUANTITATIVE DEFINITIONS OF LIKELIHOOD

An applicant may choose to provide quantitative definitions of the terms unlikely and highly unlikely. Quantitative guidelines are developed below. These guidelines serve two purposes: 1) they can be used as acceptance criteria for quantitative definitions, if provided; and 2) they provide guidance to the reviewer when objective quantitative reliability / availability information exists.

The goals from which these quantitative guidelines were derived are for specific types of accidents. Therefore the guidelines should not be used for accidents that differ significantly from these specific types. The high consequence guideline, for example, is based on a goal of no inadvertent criticalities. Thus it is only appropriate to use this guideline for accidents whose consequences are similar to a nuclear criticality accident, that is, one where a few fatal or near fatal worker doses may occur. For substantially more severe high consequence accidents, more stringent likelihood criteria would be acceptable. For less severe high consequence accidents, less stringent criteria may be applied. It should also be noted that the quantitative guidelines are derived from goals, not limits, and have been judged to be the highest values consistent with those goals.

QUANTITATIVE GUIDELINES

Quantitative guidelines have been developed because the staff will need to correlate applicant’s definitions of “highly unlikely”, “unlikely”, and “credible” with quantitative guidelines developed and used by the staff to assess compliance with 70.61. Limiting likelihood values directed by 70.61 have been quantitatively defined based on NRC strategic risk performance goals. Staff has verified that the derived values are an appropriate fraction of the risks of other industrial accident risks in the U.S., and they also conform to comparable quantitative values already used in other countries for regulation of nuclear materials facilities. The development of quantitative guidelines here does not imply that quantitative demonstration of compliance with 10 CFR 70.61 is required.

The phrase "highly unlikely" applies on a "per accident" basis. Hence, quantitative frequency guidelines for the likelihood definitions depend on how many potential accidents there are in each of the two categories.

At the time of submittal of the first ISA Summaries, the number of potential accidents in the industry will not yet be known. For review of early ISA Summaries the staff will use values of Nh and Ni[3] that are estimated to be sufficiently high to allow for the contribution not just of the one application being reviewed, but of the entire group of potential applicants. Since there are hundreds of processes in the industry, and, on the average, several accidents per process, Nh and Ni each could be on the order of 1000. If the total number of accidents identified in all the industry ISAs differs significantly from these initial assumptions, adjustments may be needed.

Highly Unlikely

The guideline for acceptance of the definition of "highly unlikely" has been derived as the highest acceptable frequency that is consistent with a goal of having no criticality accidents, and no accidents of similar consequences, in the industry. To within an order of magnitude, this is taken to mean a frequency limit of less than one such accident in the industry every 100 years. This has been translated below into a guideline limiting the frequency of individual accidents. The goal is to have no such accidents, thus it is reasonable to reduce accident frequencies substantially below these guidelines when feasible.

Unlikely

Intermediate consequence events include significant radiation exposures of workers, those exceeding 0.25 Sieverts (25 rem). It is taken as a goal that there be no increase in the rate of such significant exposures. This rate is currently about one exposure per 2.5 years. Since the uranium fuel cycle industry has not contributed to such exposures, an allocation of one tenth of this value, or 0.04 per year has been used as appropriate for this industry. Once adjusted to a per accident basis, this value of 0.04 per year for the industry becomes 0.04/Ni, and can then be used as an appropriate guideline limiting all types of accidents with intermediate consequences. This is appropriate because the defining criteria for intermediate consequence accidents in 10 CFR 70.61 were selected so that events in this category are comparable. The definition and use of the term "unlikely" submitted in the ISA Summary, to be acceptable, should be consistent with this frequency guideline.

Quantitative Guidelines for use with Acceptance Criteria

Subject to the guidance above, the applicant's quantitative definitions of the terms unlikely and highly unlikely, as applied to individual accident sequences identified in the ISA, are acceptable for showing compliance with 10 CFR 70.61 if they are reasonably consistent with the following quantitative guidelines:

Likelihood term of 70.61	guideline
unlikely	less than 0.04/Ni per year
highly unlikely	less than 0.01/Nh per year

[3] Nh is the total number of potential high-consequence accidents for the industry; and Ni is the number of intermediate-consequence accidents, as identified in the ISA's.

In setting values of these quantities, Ni and Nh, the staff should allow some added margin to account for extra accidents that may be added in the future by new facilities or processes.

It should be noted that the stated quantitative guidelines are used to define the largest likelihood values that would be acceptable limits. Definitions based on lower limits are also acceptable. The performance requirements of 10 CFR 70.61 are limits, not goals, thus staff should use these guidelines in that sense.

The quantitative consequence categories defined in 10 CFR 70.61 are broad, especially the "high-consequence" category, which is open ended. For this reason, the meaning of "highly unlikely" for an individual accident should be graded in inverse proportion to the magnitude of consequences when these consequences are significantly greater than the lower limits defining high consequences in 10 CFR 70.61.

8. INFORMATION DEMONSTRATING COMPLIANCE WITH THE PERFORMANCE REQUIREMENTS

10 CFR 70.65(b) items 3,4,6, and 8 require certain information resulting from the ISA's performed on individual processes to be described in the ISA Summary. Section 70.65(b)(4) requires that the ISA Summary contain: "information that demonstrates compliance with the performance criteria of 10 CFR 70.61." Since the requirements of 10 CFR 70.61 are expressed in terms of consequences and likelihoods of events, the information needed is that which shows that all events are of appropriate consequences and likelihood. Section 70.61 effectively states that each credible accident sequence must have a likelihood corresponding to its consequences. Thus the information submitted is acceptable if it provides consequence and likelihood information for each accident showing that:

a) credible high-consequence events are highly unlikely; and

b) credible intermediate-consequence events are unlikely.

The performance requirements of 10 CFR 70.61 have three elements: 1) completeness; 2) consequences; and 3) likelihood. Completeness refers to the fact that each credible event must be addressed. Consequences refers to the magnitude of the chemical and radiological doses used by 10 CFR 70.61 in categorizing accidents as being of high or intermediate consequences. Likelihood refers to the fact that 10 CFR 70.61 requires that intermediate consequence events be unlikely, and high consequence events be highly unlikely. Thus the information provided must address each of these three elements.

To be acceptable, the information provided must correspond to the ISA methods, consequence, and likelihood definitions described in the submittal. The information must show the basis and the results of applying these methods to each process. In addition, the information must show that the methods have been properly applied in each case.

The information showing completeness, consequences, and likelihood for accident sequences can be presented in various formats, including logic diagrams or tabular summaries. Appendix A of this chapter includes a set of tables which include the information the staff will look for in assessing the completeness, adequacy, and quality of an applicant's submittals.

Completeness is demonstrated by correctly applying an appropriate method of accident identification, as described in NUREG-1513, "ISA Guidance Document". Completeness can be

effectively displayed by using an appropriate diagram or description of the accidents identified. Specific acceptance criteria for completeness are covered in item 10 below.

Specific acceptance criteria for consequence and likelihood information follow.

Consequences

The information in the ISA Summary on consequences is acceptable for showing compliance with 10 CFR 70.61 if:

i. the information in the ISA Summary for each accident includes an estimate of its quantitative consequences (doses, chemical exposures, criticality) in a form that can be directly compared with the consequence levels in 10 CFR 70.61; or includes a reference to a value documented elsewhere in the summary that applies to or bounds that accident; and

ii. the consequences were calculated using a method and data consistent with NUREG-6410, "Nuclear Fuel Cycle Facility Accident Analysis Handbook", March 1998 or using another method described and justified in the methods description section of the ISA Summary, and

iii. all consequences that could result from the accident sequence have been evaluated. That is, if an accident can result in a range of consequences, then all possibilities must be considered, including the maximum source term and most adverse weather that could occur. However, if such conditions are unlikely to occur, credit can be taken for this in the evaluation of likelihood, and

iv. The ISA Summary correctly assigns each type of accident to one of the consequence categories of 10 CFR 70.61; namely, high, intermediate, or low (less than intermediate).

Unshielded criticality accidents are considered to be high consequence events, because there is a substantial likelihood that they would be. For processes with effective engineered shielding, criticalities may actually produce doses below the intermediate consequences of 10 CFR 70.61. As stated in the regulation, primary reliance must be on prevention of criticalities. This applies notwithstanding shielding or other mitigative features. Therefore, regardless of the actual consequences, shielded criticalities must meet the likelihood criteria described in the following section of this SRP. If needed, the Nuclear Fuel Cycle Facility Accident Analysis Handbook (NUREG/CR-6410) provides methods for estimating magnitudes of criticality events that can be applied for workers or members of the public at varying distances from the event.

Likelihood

The information in the ISA Summary is acceptable for showing compliance with 10 CFR 70.61 if:

i. The ISA Summary contains a specification of the likelihood of each type of accident sequence; and

ii. The likelihoods are derived from an acceptable method described in the ISA Summary's methods section; and

iii. The likelihoods comply with acceptable definitions of the terms "unlikely" and "highly unlikely" as described in this SRP chapter. Note that, when interpreted as required

accident frequencies, these terms refer to long-run average frequencies, not instantaneous values. That is, a system complies with the performance requirements of 10 CFR 70.61 as a long-run average. Otherwise failure of any IROFS, even for a very short period, would be a violation of the requirement, which is not the intent; and

iv. All nuclear criticality accident sequences have an evaluated likelihood of "highly unlikely", unless protected by engineered shielding and confinement; and

v. All criticality accident sequences that are protected by engineered shielding and confinement are evaluated as at least "unlikely", and none can result from a single IROFS failure. This moderately higher standard of likelihood may be permitted in preventing such events consistent with ANSI/ANS Standard 8.10. In addition, 10 CFR 70.61(d) requires that the risk of criticality must be limited by an approved margin of subcriticality for safety. Validation methods to establish margins to assure that a particular parameter value is actually subcritical, are reviewed as programmatic commitments, not as part of the ISA. However, when a safety margin is part of the reason why exceedance of safety limits is unlikely, the margin should be listed in the ISA Summary description of that accident. For example, if the process is safe against double batching, the number of batches, and other conditions, required for actual criticality should be described in the ISA Summary. The likelihood of erroneously accumulating the critical number of batches should then be reflected in the specification of the likelihood of the accident sequence.

9. PROCESS HAZARDS

The description of process hazards provided in the ISA Summary is acceptable if it identifies, for each process, all the types of hazards relevant to determining compliance with the performance criteria of 10 CFR 70.61. That is, the acceptance criterion is completeness. All hazards that were identified that could credibly result in the minimum consequences of section 70.61 should be listed, even if later analysis of a particular hazard shows that resulting accident sequences do not exceed these minima. Otherwise the reviewer cannot determine completeness. General exclusion of consideration of certain hazards for an entire facility can be justified by bounding case analyses showing that, for the conditions or credible inventories on site, the minimum consequence levels of section 70.61 cannot be exceeded. In this case, the bounding inventories or conditions, if under the control of the applicant, become IROFS. The list of process hazards is acceptable if the ISA Summary provides:

1) A list of materials (radioactive, fissile, flammable, and toxic) or conditions that could result in hazardous situations. The list includes maximum intended inventory amounts and the location of the hazardous materials at the site.

2) A hazards interaction table showing potential interactions either between materials or between materials and conditions that could possibly result in hazardous situations.

10. TYPES OF ACCIDENT SEQUENCES

The general description of types of accident sequences is acceptable if it is adequate to permit the staff to determine:

a) That all accidents that could exceed the consequence criteria of 10 CFR 70.61 have been identified, and

b) How the IROFS listed in the ISA Summary protect against each type of accident.

Types of accidents differ if they consist of a different set of failures of IROFS. Thus several processes, each using a set of IROFS that are functionally of the same type (same mechanical, physical and/or electrical principle of operation), can be summarized as a single type of accident and listed only once. However, the individual processes covered by this system should be individually identified in a way that the reviewer can determine completeness in addressing all processes.

For this reason, it is not, in general, acceptable to merely list the type of hazard, or just the controlled parameters, without reference to the items relied on to control that parameter or hazard. The general description of accident sequences is acceptable if it covers all types of sequences of initiating events and failures of IROFS (IROFS). Initiating events may be either failure of an IROFS or an external event. Human errors can be initiating events or failures of IROFS. The accident description is acceptable if it permits the staff to determine how each accident sequence that could exceed the minimum consequence levels in 10 CFR 70.61 is protected against by IROFS.

One acceptable way to do this is to show a fault tree where the basic events are failures of the IROFS. Another is to provide a table where each row displays the events in an accident sequence, as in Appendix A Table A-6, where, in general, each event is failure of an IROFS. Another acceptable way is a narrative summary for each process describing the sequence of events in each type of accident.

The general description of types of accident sequences, to show completeness, must use systematic methods and consistent references. Therefore, each description is acceptable if:

a) a method of hazard identification and process hazard analysis was used in accordance with the criteria of NUREG-1513;

b) the method selected was correctly applied;

c) no hazard or accident sequence that could cause a failure to meet section 70.61 was overlooked; and

d) a method of identifying plant processes was used, so that the completeness of the analysis in covering all processes can be evaluated.

During the early phases of an ISA, accidents will be identified whose consequences may initially be unknown. These accidents will later be analyzed and may be shown to have consequences less than the levels identified in 10 CFR 70.61 which invoke requirements. The ISA Summary must show what happened to these accidents. Thus it must identify all accidents considered, and identify accidents which, although possible, were not developed due to insufficient consequences.

It is not necessary to list as a separate sequence every conceivable permutation of the accidents. Accidents having characteristics that all fall in the same categories can be grouped as a single type of accident in the table, if:

a) the initiating events have the same effect on the system;

b) they all consist of failures of the same IROFS;

c) they all result in violation of the safety limit on the same parameter; and

d) they all result in the same type and severity categories of consequences.

11. DESCRIPTIVE LIST OF ALL IROFS

The "list describing items relied on for safety" required by 10 CFR 70.62(c)(vi) is acceptable if:

1) It includes all IROFS in the identified accident sequences.

2) The description of the IROFS, the identification of the grade of management measures applied to them, and the associated safety limits and margins is adequate to permit a determination of compliance with 10 CFR 70.61, that is, it includes the characteristics of its preventive, mitigative, or other safety function, and the assumptions and conditions under which the item is relied upon to support compliance with the performance requirements of Sec. 70.61.

Although the regulations do not explicitly list the content and grading of management measures as a separate element of an ISA Summary, such information is required to "demonstrate compliance with the performance requirements" by the IROFS. Normally this information would be available in the current license application. If sufficiently detailed information is not provided in the current application, submittal of additional information may be required.

The above acceptance criteria are explained in greater detail below.

1) ALL ITEMS: The primary function of the "list describing all items relied on for safety" is to document the safety basis of all processes in the facility. This list assists in assuring that the items are not degraded without a justifying safety review. Thus the key feature of this list is that all IROFS are included. To be acceptable, no item, aspect, feature, or property of the processes that is needed to show compliance with the safety performance requirements of the regulation may be left off this list. IROFS may be hardware with a dedicated safety function or hardware with a property that is relied on for safety. Thus IROFS may be the dimension, shape, capacity, or composition of hardware. In some processes, the frequency of demands made on IROFS must be controlled or limited to comply with 10 CFR 70.61. In such processes, whatever features are needed to limit the frequency of demands are themselves IROFS.

2) THE DESCRIPTIONS OF ITEMS: The essential features of each item relied on for safety (IROFS) that are required to achieve adequate reliability should be described. Sufficient information should be provided about engineered hardware controls to permit an evaluation that, in principle, controls of this type will have adequate reliability. Because the likelihood of failure of items often depends on safety margins, the safety parameter controlled by the item, the safety limit on the parameter, and the margin to true failure should, in general, be described. For IROFS that are administrative controls, the nature of the action or prohibition involved must be described sufficiently to permit an understanding that, in principle, adherence to it should be reliable. Features of the IROFS that affect its independence from other IROFS, such as reliance on the same power supplies, should be indicated.

The description of each item must contain any information needed to identify how the management measures, such as maintenance, training, configuration management,

etc. are applied to it. If a system of graded management measures is used, the grade applied to each control should be determinable from information provided. Section 70.62(d) requires that applicants "...establish management measures to provide continuing assurance of compliance with the performance requirements of Sec. 70.61". The reliability required for an IROFS is proportionate to the amount of risk reduction relied on. Thus the quality of the management measures applied to an IROFS may be graded commensurate with the reliability required. The management measures shall assure that IROFS are designed, implemented, and maintained, as necessary, to be available and reliable to perform their function when needed. The degree of reliability and availability of IROFS assured by these measures should be consistent with the evaluations of accident likelihoods. In particular, for redundant IROFS, all information necessary to establish the average vulnerable outage time is required in order to maintain acceptable availability. Otherwise failures must be assumed to persist for the life of the plant. In particular, the time interval between surveillance observations or tests of the item should be stated, since restoration of a safe state can not occur until the failure is discovered.

One example of a tabular description of IROFS meeting these criteria is Table A-12 in Appendix A.

12. LIST OF SOLE ITEMS RELIED ON FOR SAFETY (IROFS)

The descriptive list that identifies all IROFS that are the sole item for preventing or mitigating an accident sequence is acceptable if it includes:

a) A descriptive title of the item;

b) Provides an unambiguous and clear reference to the process to which the item applies; and

c) Provides a clear and traceable reference to the description of the item as it appears in the full list of all items.

13. INFORMATION DEMONSTRATING COMPLIANCE WITH THE REQUIREMENTS OF 10 CFR 70.24 FOR CRITICALITY MONITORING

10 CFR 70.24 has specific sensitivity requirements for criticality monitors. To demonstrate compliance, the method for evaluating an acceptable response of at least two detectors to a criticality at any location where SNM may be handled, used, or stored should be described. Locations of all detectors relative to the potential locations of SNM should be provided as a diagram. Information supporting determination of the gamma and neutron emission characteristics of the minimum credible accident of concern capable of producing the effects specified in 10 CFR 70.24 should be provided. Actual neutron and gamma doses and dose rates at the detector locations should be given. Information showing the response characteristics of the detectors to neutron and gamma doses and rates characteristic of credible accidents should be given.

10 CFR 70.24 also requires specific emergency preparations. Information should be provided demonstrating that equipment and procedures of the applicant are adequate to assure that these requirements are met.

14. INFORMATION DEMONSTRATING COMPLIANCE WITH REQUIREMENTS OF 10 CFR 70.64 FOR NEW FACILITIES

10 CFR 70.64 specifies baseline design criteria that must be used, as applicable, for new facilities and new processes at existing facilities. If the application involves such new facilities or process, then an acceptable set of information would address each baseline design criterion listed in 10 CFR 70.64, and would show how the criterion is met. For criteria such as double contingency to which each individual process must comply, the process-specific information may be provided along with the other process information in the ISA Summary. Design basis events and safety parameter limits should be given. Methods, data, and results of analysis showing compliance with these design bases should be given for individual processes and structures.

10 CFR 70.64 states that the design process must be based on defense-in-depth principles, and must incorporate, to the extent practicable, preference for engineered controls over administrative and reduction of challenges to IROFS. Because of this regulation, new facilities with system safety designs lacking defense-in-depth, or consisting of purely administrative controls, or relying on IROFS that are frequently or continuously challenged are not acceptable unless justification is provided showing that alternatives achieving the design criteria are not feasible.

3.5 REVIEW PROCEDURES

Organization of the reviews addressed by this SRP will differ depending on the scope of the documents submitted. For a license application, renewal, or amendment application containing a new or revised chapter addressing Safety Program and ISA commitments there may only be a primary ISA reviewer. However, for an initial ISA Summary submittal, this primary ISA reviewer will be assisted by specialists in the various safety disciplines and management measures. An ISA Summary update submitted as part of an amendment for a process that has hazards in multiple disciplines would also require a team approach. In general, there will be a primary ISA reviewer who evaluates generic methods, risk and reliability criteria used in the ISA, and generic information about individual processes. This primary reviewer will be assisted by secondary reviewers who evaluate selected individual accidents, and advise on the completeness of the accident list for specific safety disciplines.

3.5.1 Acceptance Review

For an ISA programmatic application, amendment, or ISA Plan, the primary ISA reviewer will conduct a review to determine if the submittal contains appropriate information addressing each of the areas of review identified in Section 3.3.1 of this chapter. If the application does not contain sufficient information addressing the areas of review to permit a safety evaluation, then the application will not be accepted.

For an ISA Summary, the primary ISA reviewer will also conduct an acceptance review to determine whether the document submitted contains sufficient information addressing the Areas of Review noted in section 3.3.2, including specifically each of the elements required by 10 CFR 70.65(b), to permit an evaluation of safety for compliance with the regulations. If insufficient information is not present, the ISA Summary will not be accepted.

3.5.2 Safety Evaluation

3.5.2.1 Evaluation of Safety Program and ISA Commitments

The staff reviews the descriptions and commitments to program elements in the application or other documents in the subject areas described in Section 3.3.1 to ascertain whether the program elements are sufficient to meet the acceptance criteria of section 3.4.3.1. The information addressing the subject areas listed in 3.3.1 may be contained in the ISA Chapter of a license application, renewal or amendment; or in the ISA approach described in an ISA Plan submitted in accordance with 70.62(c)(3)(i). Part of the information required to evaluate these areas may also be found in chapters of a license application other than the ISA chapter. ISA is highly interrelated with all other aspects of a safety program. Hence the ISA reviewer must co-ordinate with reviews being conducted under other chapters of this SRP. Specific review steps correspond closely to the areas of review in section 3.3.1.

3.5.2.2 Evaluation of ISA Summary and Results

Evaluation of the ISA Summary to determine if the acceptance criteria of section 3.4 have been met would normally be performed by a team consisting of a primary ISA reviewer together with specialists in each category of accidents. These categories of accidents depend on the facility, but, in general, are: nuclear criticalities, fires, chemical accidents, and radiological accidents. If external event analysis is complex, specialists may be employed to review these separately as well. The primary ISA reviewer would normally evaluate the acceptability of the generic elements of the ISA Summary, such as site and facility descriptions, ISA methods, criteria, and consequence and likelihood definitions. However, each specialist should also review these elements to obtain information in support of their own evaluations.

In contrast to these generic ISA elements, process-specific information is needed by, and must be acceptable to, all of the specialists. Thus the process descriptions in the ISA Summary should be evaluated by all of the team members.

Reviews of accident sequence descriptions and the likelihood and consequence information showing compliance with Section 70.61 should be done by separate specialists for each category of accidents. These accident categories are: nuclear criticalities, fires, radiological releases, and chemical accidents. As indicated in Appendix A, one acceptable format for the ISA Summary is to tabulate or give logic diagrams for accident sequences in each of these groups separately.

After a preliminary team review of the ISA Summary, a visit to the facility would normally be made for familiarization with the 3-D geometry of process equipment and other information.

Selection of specific accident sequences and IROFS for more detailed evaluation should then be made using the following approach. The staff will evaluate the risk significance of accident sequences using information supplied in the ISA Summary. The applicant's own method for evaluating significance may provide information sufficient for this purpose. If not, the NRC staff may make an evaluation of risk significance using risk indexing, or similar qualitative screening criteria, analogous to Table A-6 in Appendix A. One such procedure for evaluating risk significance is described in the last section of Appendix A. Other, more rigorous reliability or consequence analyses may be performed as judged necessary. Based on this risk screening, accident sequences will be placed in risk categories. Engineered and administrative controls appearing in those sequences in the category of highest risk significance may be selected for review in greater detail. Independent evaluation of these sequences, or site visits, will be

performed, if warranted. From accident sequences categorized as of lower risk significance, staff will select a small sample of representative sequences for specific evaluation.

For the list describing the IROFS, the reviewer should categorize IROFS so that items of a similar nature, and similar risk significance, are grouped together. The reviewer should then assure that he has a full understanding of one or more prototype IROFS selected from each category. For these selected prototypes, the reviewer may, if necessary, request additional information to reach such a full understanding of particular IROFS. For complex processes, it may be necessary to visit the plant to reach an adequate understanding of how the IROFS work for the process.

3.6 EVALUATION FINDINGS

The reviewer verifies that the information submitted by the applicant is sufficiently complete so that compliance with the regulations can be evaluated. For each requirements statement in the regulation addressing ISA, the evaluation findings should include a brief statement as to why the information submitted demonstrates compliance. There should be a finding statement, following the evaluation of each area of review, stating how the information submitted in that area supports the related regulatory requirement. Specifically, the staff findings in the SER should state conclusions of the following types:

General conclusion resulting from staff evaluation of safety program commitments:

> The staff concludes that the applicant's safety program, if established and maintained pursuant to Sec. 70.62 is adequate to ensure that each item relied on for safety will be available and reliable to perform its intended function when needed and in the context of the performance requirements of 10 CFR 70.61.

There should be general findings, for each of the areas of review, stating how the applicant's information demonstrates compliance with the acceptance criteria of section 3.4.3.1. If staff finds that the acceptance criteria are not met, a license condition rectifying the deficiency should be recommended. If the applicant has submitted an adequate explanation of an alternative way of complying with the regulations, the staff evaluation should contain a finding that the alternative is acceptable for meeting the basic regulatory requirement addressed.

General conclusions resulting from staff evaluation of an ISA Summary:

> Many hazards and potential accidents can result in unintended exposure of persons to radiation, radioactive materials, or toxic chemicals associated with licensed materials. The staff finds that the applicant has performed an Integrated Safety Analysis (ISA) to identify and evaluate those hazards and potential accidents as required by the regulations. The staff has reviewed the ISA Summary and other information, and finds that it provides reasonable assurance that the applicant has identified items relied on for safety and established engineered and administrative controls to ensure compliance with the performance requirements of 10 CFR 70.61. Specifically, the staff finds that the ISA results, as documented in the ISA Summary, provides reasonable assurance that the IROFS, the management measures, and the licensee's programmatic commitments will, if properly implemented, make all credible intermediate consequence accidents unlikely, and all credible high consequence accidents highly unlikely.

Findings should be made concerning any specific requirements statements in 10 CFR 70 that address the 14 elements in the ISA Summary. In particular, these findings should include

statements concerning compliance with the requirements of 10 CFR 70.64 (regarding new facilities and new processes at existing facilities) for those processes to which they are applicable.

Findings may be made concerning compliance of specific processes with requirements of section 70.61 or other parts of the regulation, for those processes which receive specific detailed review. However, such findings should be limited to a finding of reasonable assurance that a process having the items relied on for safety, as described in the ISA Summary, is capable of meeting the requirements, if properly implemented, operated, and maintained.

3.7 REFERENCES

American Institute of Chemical Engineers (AIChE), “Guidelines for Hazard Evaluation Procedures, Second Edition with Worked Examples,” New York, September 1992.

American National Standards Institute, American Nuclear Society, "Nuclear Criticality Safety in Operations With Fissionable Materials Outside Reactors," ANSI/ANS-8.1-1983, La Grange Park, IL, 1983.

U.S. Code of Federal Regulations , Title 10, Part 70, Domestic Licensing of Special Nuclear Material, U.S. Government Printing Office, Washington, DC.

U.S. Department of Commerce, Bureau of the Census, “Statistical Abstract of the United States,” Table No. 688, 1995.

U.S. Nuclear Regulatory Commission, “Integrated Safety Analysis Guidance Document,”NUREG-1513, 1995.

APPENDIX A

EXAMPLE PROCEDURE FOR RISK EVALUATION

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

This appendix describes one method of evaluating compliance with the consequence-likelihood performance requirements of 10 CFR 70.61. The method is intended to permit quantitative information to be considered, if available. For consistency, the staff's approach could also include assigning quantitative values to any qualitative likelihood assessments made by the licensees since likelihoods are inherently quantitative. This method should not be interpreted as requiring that an applicant use quantitative evaluation. However, evaluation of a particular accident should be consistent with any facts available, which may include quantitative information, concerning the availability and reliability of controls involved.

The method of this appendix describes both qualitative and quantitative criteria for evaluating frequency indices of safety controls. These criteria for assigning indices, particularly the descriptive criteria in Tables A-8 and A-9, are intended to be examples, not universal criteria. It is preferable that such criteria be developed by each applicant based on the particular types of controls and management measure programs in the facility evaluated. Such criteria should be modified and improved as insights are gained during performance of the ISA.

The procedure described in this appendix is one method by which the applicant may use the ISA results to demonstrate that the requirements of 10 CFR 70.61 have been met. If the licensee evaluates accidents using a different method, the method should produce similar results in terms of how accidents are categorized. This method should be regarded as a screening method, not as a definitive method of proving the adequacy or inadequacy of the controls for any particular accident. Because methods can rarely be universally valid, individual accidents for which this method does not appear applicable may be justified by an evaluation using other methods. The method does have the benefit that it evaluates, in a consistent manner, the characteristics of controls used to limit accident sequences. This will permit identification of accident sequences with defects in the combination of controls used. Such controls can then be further evaluated or improved to establish adequacy. The procedure also ensures the consistent evaluation of similar controls by different ISA teams. Sequences or controls that have risk significance, and are evaluated as marginally acceptable, are good candidates for more detailed evaluation by the applicant and the reviewer.

The tabular accident summary resulting from the ISA should identify, for each sequence, what engineered or administrative controls must fail to allow the occurrence of consequences that exceed the levels identified in 10 CFR 70.61. Chapter 3 of this SRP specifies acceptance criteria for these controls, such that the performance requirements of section 70.61 are met. These criteria require that controls be sufficiently unlikely to fail. However, the acceptance criteria do not explicitly mandate any particular method for assessing likelihood. The purpose of

this appendix is to provide an example of an acceptable method to perform this evaluation of likelihood.

A.1 DETERMINING COMPLIANCE WITH GRADED PROTECTION REQUIREMENTS

Section 70.61 of 10 CFR Part 70 describes requirements for a system of protection sufficient to limit the risk of identified accidents by making accidents of higher potential consequences have a proportionately lower likelihood of occurrence. The regulation specifies two categories of consequences into which an accident may fall. The first category is referred to in 10 CFR 70.61 as "high consequences", and the second as "intermediate consequences". Implicitly there is a third category; 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 uncontrolled and unmitigated accidents having consequences that exceed the levels in section 70.61, it will, in some cases, identify uncontrolled and unmitigated accidents accidents that produce radioactive or chemical exposures,that do not exceed the threshold values for intermediate consequences. For this reason, in the method described here, the table listing accidents is intended to include such low consequence accidents in order to show that they have been considered. If they are not listed, some other demonstration of the completeness of the accident identification task should be provided in the ISA Summary.

The limits defining the three accident consequence categories are given below. Note that the categories are numbered in ascending order of the magnitude of their consequences. The usefulness of this numbering will be evident later. The symbols AEGL and ERPG refer to chemical exposure levels from accidents sufficient to produce certain effects. AEGL-3 and ERPG-3 levels are life threatening. 10 CFR 70 does not specify the use of AEGL or ERPG levels. 10 CFR 70.61(b) and (c) require applicants to propose quantitative exposure levels that they would use in the two primary consequence categories below. AEGL and ERPG levels are acceptable for those substances for which the levels have been determined by the appropriate agencies, and are described here.

Consequence Category 3- High Consequences: An accident resulting in any consequence specified in 10 CFR 70.61(b). These include acute worker exposures of 1 Sievert (100 rem)[1] or greater Total Effective Dose Equivalent (TEDE), chemical exposures that could endanger the life of a worker (above AEGL-3 or ERPG-3); or acute exposures to members of the public outside the controlled area from a radiation dose of 0.25 Sievert (25 rem) or greater TEDE, a 30 mg soluble uranium intake, or chemical exposures that could lead to irreversible or other serious long-lasting health effects (exceeding AEGL-2 or ERPG-2).

Consequence Category 2- Intermediate Consequences: An accident resulting in any consequence specified in 10 CFR 70.61(c). These include acute exposures of workers to a radiation dose between 0.25 Sievert and 1 Sievert TEDE, or chemical exposures that could lead to irreversible or other serious long-lasting health effects (above AEGL-2 or ERPG-2); or acute exposures of members of the public outside the controlled area to a radiation dose between 0.05 and 0.25 Sievert TEDE, or chemical exposures that could cause mild transient health effects (exceeding AEGL-1 or ERPG-1); or prompt release of radiation outside the restricted

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

area that would, if averaged over a 24 hour period, exceed 5000 times the values specified in Table 2 of Appendix B to 10 CFR Part 20.

Consequence Category 1- Low Consequences: Any accident with potential adverse radiological or chemical consequences but at exposures less than Categories 3 and 2 above.

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

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

	Workers	Offsite Public	Environment
Consequence Category 3: high	D>1 Sv (100 rem) >AEGL3, ERPG3	D>.25 Sv (25 rem) 30 mg sol U intake >AEGL2, ERPG2	
Consequence Category 2: intermediate	.25 Sv<D≤ 1 Sv >AEGL2, ERPG2 but <AEGL3, ERPG3	.05 Sv<D≤ .25 Sv >AEGL1, ERPG1 but <AEGL2, ERPG2	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 70.61 (Categories 2 and 3 in Table A-1), engineered and administrative controls and management measures must be provided sufficient to ensure that the likelihoods of these adverse events are correspondingly low. The categories of likelihood are shown in Table A-2.

Table A-2: Likelihood Categories Based on 10 CFR 70.61

	Qualitative Description
Likelihood Category 1	Consequence Category 3 accidents must be "highly unlikely"
Likelihood Category 2	Consequence Category 2 accidents must be "unlikely"
Likelihood Category 3	"Not unlikely"[2]

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

A major purpose of the ISA is to show compliance with the above system of graded protection. This can be done by using the required tabular summary of identified accident sequences. One acceptable way of doing so is for the applicant to assign two category numbers to each of these accident sequences with the system of protection in place, one based on its consequences and one for likelihood. The product of these two category numbers is then used as a risk index. Listing this calculated risk index in the tabular summary provides a simple method for showing that the graded protection requirements have been met for each accident sequence. A risk index value less than or equal to "4" means the sequence is acceptably protected and/or mitigated. If the applicant provides this risk index in one column of the tabular summary, the reviewer can quickly scan this column to confirm that each accident conforms to the safety performance requirements of 10 CFR 70.61. This system is equivalent to assigning each protected and/or mitigated accident to a cell in a 3 by 3 matrix. This conceptual matrix is shown in Table A-3 below. The values in the matrix cells are the risk index numbers.

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

Table A-3: Risk Matrix with Risk Index Values

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

To demonstrate compliance with the system described above, the applicant needs to assign consequence categories to each identified accident 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, the controlled and/or mitigated accident consequences and likelihoods must have valid bases, and the applicant must demonstrate the bases in the ISA Summary.

A.2 CONSEQUENCE CATEGORY ASSIGNMENT

The assignment of consequence categories is based on estimated consequences of prototype accidents. 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", March 1998, describes valid methods and data that may be used by the applicant, or by the staff for confirmatory evaluations.

A.3 LIKELIHOOD CATEGORY ASSIGNMENT

An assignment of an accident sequence to a likelihood category is acceptable if it is based on the record of failures at the facility or other methods that have objective validity. Because sequences leading to accidents often involve multiple failures, a combination of failure frequency and probability values determines the likelihood of the whole sequence. These values include the frequencies of initiating events and failure likelihoods of engineered and administrative controls. An acceptable method is described below by which the applicant can make an estimate of an approximate likelihood category for an accident sequence by considering all the events involved. This method makes use of the number, type, independence, and observed failure history of controls, as evaluated by an applicant using

expert engineering judgement. Thus, a reasonably accurate evaluation of the appropriate estimated likelihood of accidents using such a qualitative system depends on the informed judgement of the analyst. Engineered and administrative controls, even those of the same types, have a wide range of reliability. The ultimate criterion for acceptability is that the frequencies of initiating events and the likelihoods of failure of controls involved are sufficiently low so that the entire accident sequence is "highly unlikely" or "unlikely" as required by 10 CFR 70.61. The virtue of the method is that it requires explicit consideration of most of the underlying events and factors that significantly affect the likelihood of the accident. Another virtue is that the use of explicit criteria to assign likelihood yields more consistent results across different systems within a plant and among different applicants.

Underlying any evaluation of an accident sequence as "unlikely" or "highly unlikely" is an implied assessment of its "likelihood" or frequency of occurrence. The method described below will indicate which likelihood category may be appropriate for an event. In order to maintain internal consistency in evaluating different control systems and accidents, it was necessary to derive this method based on the underlying frequencies of events. The numerical guidelines contained in Table A-4 below were thus used to obtain consistency and to be consistent with staff safety goals.

Table A-4: Event Likelihood

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

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

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

Similarly, accident sequences having frequencies more than 10^{-4} per year per accident are not considered "unlikely." Again this value should not be taken as a definitive criterion for

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

The accident evaluation method described below does not preclude the need to comply with the double contingency principle for sequences leading to criticality. Although exceptions are permitted with compensatory measures, double contingency, should, in general, be applied. The reason 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 have at least 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 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 be unlikely.

A.4 QUALITATIVE CATEGORIZATION OF IROFS

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

Reviewers should note that the coarse qualitative criteria for evaluation of controls (IROFS) in Tables A-5, A-8, and A-9 are given as illustrations only. IROFS meeting the criteria for a particular score in these tables could have a wide range of availability or reliability. Such coarse criteria are useful for screening purposes; but, when the total evaluated likelihood score for an accident sequence lies near the acceptance guideline value, then a more careful evaluation should be done. Such evaluations should consider the management measures applied to all the reliability and availability qualities of the set of IROFS protecting against the accident, as explained in the likelihood acceptance criteria of this chapter in section 3.4.3.2 subsections 5 and 7.

Table A-5: Qualitative Categorization of IROFS

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

A.5 ASSESSING EFFECTIVENESS OF IROFS

The risk of an accident sequence is reduced through application of different numbers and types of IROFS. By either reducing the likelihood of occurrence or by mitigating its consequences, IROFS can reduce the overall resulting risk. The designation of IROFS should generally be made to reduce the likelihood (i.e., prevention of an accident), but the consequences may also be reduced by minimizing the potential hazards (e.g., quantity) if practical. Based on hazards identification and accident analyses where the resulting unmitigated or uncontrolled risks are unacceptable, key safety controls (administrative and/or engineered controls) may be designated as IROFS to reduce the likelihood of occurrence and/or mitigate the consequence severity.

A.6 RISK INDEX EVALUATION SUMMARY

As previously mentioned, an acceptable way for the applicant to present the results of the ISA is a tabular summary of the identified accident sequences. Table A-6 is an acceptable format for such a table. This table lists several example accident sequences for a powder blender at a typical facility. Table A-6 summarizes two sets of information: (1) the accident sequences identified in the ISA; and (2) a risk index calculated for each sequence to show compliance with the regulation. A summary of the risk index calculation will be given below.

Accident sequences result from initiating events, followed by failure of one or more controls. Thus there are columns in Table A-6 for the initiating event and for controls. Controls may be mitigative or preventive. Mitigative controls are measures that reduce the consequences of an accident. The phrase “uncontrolled and/or unmitigated consequences” describes the results when the system of preventive controls fails and mitigation also fails. Mitigated consequences result when the preventive controls fail, but mitigative measures succeed. These are abbreviated in the table as “unmit.” and “mitig.”, respectively. Index numbers are assigned to

initiating events, control failure events, and mitigation failure events, based on the reliability characteristics of these items.

With redundant 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 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, depending on the number of events involved, 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-7.

The values of index numbers in sequences are assigned considering the criteria in Tables A-8 through A-10. Each table applies to a different type of event. Table A-8 applies to events that have frequencies of occurrence, such as initiating events and certain control failures. When failure probabilities are required for an event, Table A-9 provides the index values. Table A-10 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 vulnerable to failure of the second. This period of vulnerability can be terminated in several ways. The first failure may be "fail-safe". The first failure may be continuously monitored, thus alerting the operator when it fails so that the system may be quickly placed in a safe state. Or the controls may be subject to periodic surveillance tests for hidden failures. When hidden failures are possible, these surveillance intervals limit the duration that the system is in a vulnerable state. The reverse sequences, where the second control fails first, should be considered as a separate accident sequence. This is necessary because the failure frequency and the duration of outage of the second control may differ from that of the first. The values of these duration indices are not merely judgmental. They are directly related to the time intervals used for surveillance, and the time needed to render the system safe.

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

For all these index numbers, the more negative the number is, the less likely is the failure. Accident sequences may consist of varying numbers of events, starting with an initiating event. The total likelihood index is the sum of the indices for all the events in the sequence, including those for duration.

Consequences are assigned to one of the three consequence categories of the Risk Matrix based on calculations or estimates of the actual consequences of the accident sequence. The consequence categories are based on the levels identified in 10 CFR 70.61. Multiple types of consequences can result from the same event. The consequence category is chosen for the most severe consequence.

As shown in the first row of Table A-6, the failure duration index can make a large contribution to the total likelihood index. Therefore, the reviewer should verify that there is adequate justification that the failure will be corrected in the time ascribed to the duration index. In general, duration indices with values less than minus one (-1), corresponding to 36 days, to be acceptable, should be based on the existence of intentional monitoring of the process. The duration of failure for an unmonitored process should be conservatively estimated.

Table A-6 provides two risk indices for each sequence in order to permit evaluation of the risk significance of the controls involved. To measure whether a control has high risk significance, the Table provides an "uncontrolled risk index", determined by modeling the sequence with all controls as failed (i.e., not contributing to a lower likelihood). In addition, a "controlled risk index" is also calculated, taking credit for the low likelihood and duration of control failures. When an accident sequence has an uncontrolled risk index exceeding 4, but a controlled index of less than 4, then the controls involved have a high risk significance in that they are relied on to achieve acceptable safety performance. Thus use of these indices permits evaluation of the possible benefit of improving controls, and also whether a relaxation may be acceptable.

Table A-11 provides a more detailed description of the accident sequences used in the example of Table A-6. The reviewer needs the information in Table A-11 to understand the nature of the accident sequences listed in Table A-6. Table A-6 lacks sufficient room to explain any but the simplest failure events.

Table A-12 is used to explain the controls and external initiating events that appear in the accident sequences in Table A-6. The reviewer needs the information in Table A-12 to understand why the initiating events and controls listed in Table A-6 have the low likelihood indices assigned. Thus Table A-12 needs to address such information as: 1) the margins to safety limits, 2) the redundancy of a control, and 3) the measures taken to assure adequate reliability of a control. Table A-12 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-6: Example Accident Sequence Summary And Risk Index Assignment

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

Accident	Initiating Event (a)	Preventive Control 1 (b)	Preventive Control 2 (c)	Mitigation Control (d)	Likelihood* Index T (e) uncontrolled controlled	Likelihood Category (f)	Conse quence Evaluation Reference	Conse-quence Category (g)	Risk Indices (h=f x g) uncontrolled controlled	Comments & Recommendations
PPB2-1A (Criticality from blender leak of UO_2)	see Control 1 (note 1)	PPB2-C1: Mass Control Failure: Blender leaks UO_2 onto floor, critical mass exceeded frq1 = -1 dur1 = -4	PPB2-C2: Moderation Failure: Suffic. water for criticality introduced while UO_2 on floor frq2 = -2	N/A	unc T = -1 con T = -7	unc 3 con 1	rad 35	3 (crit: 3, rad: 0)	9 3	criticality, consequences = 3 Control 2 fails while Control 1 is in failed state. T = -1-4-2 = -7
PPB2-1B (Rad. release from blender leak of UO_2)	blender leaks UO2 frqi = -1	PPB2-C1: Mass Control success: leaked UO_2 below critical mass, OR	PPB2-C2: Moderation success: no moderator	Ventilation Failure: Ventilated blender enclosure prf = -3	unc T = -1 con T = -4 con T = -1	unc 3 unmit. 2 mitig. 3	rad 36	unc 2 unmit. 2 mitig. 1	6 unmit. 4 mitig. 3	rad consequences, no criticality unmitigated sequence: control 1 & mitigation fail. T= -1-3 = -4 mitig.: Control 1 fails, mitig. control does not fail. T = -1
PPB2-1C	see Control 1 (note 1)	PPB2-C2: Moderation Failure: Suffic. water for criticality on floor under UO_2 blender frq1 = -2 dur1 = -3	PPB2-C1: Mass Control Failure: Blender leaks UO_2 on floor while water present frq2 = -1	N/A	unc T = -2 con T = -6	unc 2 con 1	rad 35	3 (crit: 3, rad: 0)	6 3	criticality by reverse sequence of PPB2-1A, moderation fails first. Note different likelihood T = -6
PPB2-2	Fire in Blender Room frqi = -2	Fire Suppression Failure: Fails on demand: prf1 = -2	N/A	N/A	unc T = -2 con T = -4	unc 2 con 2	rad 37	2 (rad) 1	4 2	Event sequence is just initiating event plus one control failure on demand

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

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

Table A-7: Determination of Likelihood Category

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

Table A-8: Failure Frequency Index Numbers

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

* Indices 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 index value 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. Criteria justifying assignment of the lower (more negative) value should be given in the narrative describing ISA methods. Exceptions require individual justification.

Table A-9: 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 (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 control have been observed to fail.
-3 or -4*	10^{-3} - 10^{-4}	A single passive engineered ctrl. (PEC) or an active engineered control (AEC) with high availability	
-2 or -3 *	10^{-2} - 10^{-3}	A single active engineered control, 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	

* Indices 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.

Table A-10: Failure Duration Index Numbers

Duration Index Number	Avg. Failure Duration	Duration in Years	Comments
1	More than 3 years	10	
0	1 year	1	
-1	1 month	0.1	Formal monitoring to justify indices less than “-1"
-2	A few days	0.01	
-3	8 hours	0.001	
-4	1 hour	10^{-4}	
-5	5 minutes	10^{-5}	

Table A-11: Accident Sequence Descriptions

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

Accident (see Table A-6)	Description
PPB2-1A Blender UO_2 leak criticality	The initial failure is a blender leak of UO_2 that results in a mass sufficient for criticality on the floor. (This event is not a small leak.) Before UO_2 can be removed, moderator sufficient to cause criticality is introduced. Duration of critical mass UO_2 on floor estimated to be one hour.
PPB2-1B Blender UO_2 leak, rad. release	The initial failure is a blender leak of UO_2 that results in a mass insufficient for criticality on the floor, or mass sufficient for criticality but moderation failure does not occur. Consequences are radiological, not a criticality. A ventilated enclosure should mitigate the radiological release of UO_2. If it fails during cleanup or is not working, unmitigated consequences occur.
PPB2-1C	The events of PPB2-1A occur in reverse sequence. The initial failure is introduction of water onto the floor under the blender. Duration of this flooded condition is 8 hours. During this time, blender leaks a critical mass of UO_2 onto the floor. Criticality occurs.
PPB2-2	Initiating event is a fire in the blender room. Fire is not extinguished in time. Release of UO_2 from process equipment occurs. Offsite dose estimated to exceed 100 mrem.

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

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

Safety Control Identifier	Safety Parameter and Limits	Safety Controls Description	Max Value of Other Parameters	Reliability Management Measures	QA Grade
PPB2-C1	Mass Outside Hopper: zero	Mass Outside Hopper: Hopper and outlet design prevent UO_2 leaks, double gasket at outlet.	Full Water Reflection, Enrichment 5%	Surveillance for leaked UO2 each shift	A
PPB2-C2	Moderation: in UO_2 < 1.5 wt. % External Water in area: zero	Moderation In UO_2 : Two sample measurements by two persons before transfer to hopper. External Water: Posting excluding water, double piping in room, floor drains, roof integrity	Full Water Reflection, Enrichment 5%	Drain, roof, and piping are under safety grade maintenance	A

Note: In addition to engineered controls, this table should include descriptions of external initiating events whose low likelihood is relied on to achieve acceptable risk, especially those which are assigned frequency indices lower than -4. The descriptions of these initiating events should contain information supporting the frequency index value selected by the applicant.

ACCIDENT SUMMARY AND RISK INDEX ASSIGNMENT FOR TABLE A-6

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

Accident Sequence

This column is provided to list the accident sequences identified by the applicant in the ISA Summary. It is important to the proper documentation of the ISA that the applicant subdivides the plant 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 "Blender Hopper" node described In Table **A-6** has the unique identifying symbol PPB2. Additional identifier characters have been added to form the identifier, PPB2-1, to identify the first accident sequence identified in that node. Because the applicant should list all the plant controls of significance used elsewhere in the ISA, tabulations of the unique node (and accident) identifier can be used to find the accidents that these controls 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.

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 exceeding those identified in 70.61. Initiating events are of several distinct types: (1) external events, such as hurricanes and earthquakes, (2) plant events external to the node being analyzed (e.g., fires, explosions, failures of other equipment, flooding from plant water sources), (3) deviations from normal of the process in the node (i.e., credible abnormal events), and (4) failures of controls of the node. The tabulated initiating events should only consist of those that involve an actual or threatened failure of controls, or that cause a demand requiring controls to function in order to prevent consequences exceeding 70.61 levels. The frequency index number for initiating events is referred to in the table using the symbol "frqi". Table A-8 provides criteria for assigning a value to frqi. Usually, insufficient room is present in a tabular presentation like Table A-6 to describe accurately the events indicated. Consequently, the applicant should provide supplementary narrative information to adequately describe each accident sequence of Table A-6. Cross referencing between this information and the table should be adequate, for instance, the unique symbolic accident sequence identifiers can be used. Table A-11 is an example of a list of supplementary accident sequence descriptions corresponding to Table A-6.

Preventive Control 1

This column is provided to list a control designed to prevent consequences exceeding 70.61 levels. If separate controls are used to prevent different consequences, separate rows in the table should be defined corresponding to each type of consequence. Table A-6 contains an example of a set of related sequences so separated. Sequences where two controls must simultaneously be in a failed state require assignment of three index numbers: the failure frequency of the first control, frq1, the duration of this failure, dur1, and the failure frequency of the second control, frq2. For such sequences, the initiating event is failure of the first control. In these cases, frq1 is assigned using Table A-8. The failure duration of the first control is assigned using Table A-10. 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-9. The symbol "b" is used in the column heading for the indices associated with this control.

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.

Mitigation Control
This column is provided in case controls are available to mitigate the accident. That is, they reduce, but do not eliminate, the consequences of a sequence. A control that eliminates all adverse consequences should be considered preventive. The symbol “d” is used in the column heading for the indices associated with this control.

Likelihood 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-7. The symbol “e” is used for this category number in the column heading.

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

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 10 CFR 70.61. The symbol “f” is used for this category number in the column heading. Sequences having controls to mitigate consequences must be divided into two cases, one where the mitigation succeeds, and one where it fails, each with different consequences. The two cases may be tabulated in one row of Table A-6, but the mitigated and unmitigated consequences should be separately indicated. Unless the mitigated case results in consequences below those levels identified in 10 CFR 70.61, both cases must satisfy the likelihood requirements as shown by the risk matrix.

Risk Index
This column is provided to list the risk index, which is calculated as the product of the likelihood category and consequence category numbers. This is shown in the column heading by the formula “g = e x f”. Sequences with values of “g” less than or equal to “4" are acceptable. Another risk index can also be calculated as the product of the consequence category number times the likelihood category associated with only the failure frequency index for the initiating event. The resulting product can be referred to as the “unmitigated” risk index. It is unmitigated in the sense that no credit is taken for the functioning of any subsequent controls. For example, in the first three cases in Table A-6, the initiating event is failure of Preventive Control 1. In these cases, the failure frequency of Preventive Control 1 is used to determine the likelihood category when calculating the unmitigated risk index.

Comments and Recommendations
This column is needed to record ISA team recommendations, especially when the existing system of 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.

DETERMINATION OF LIKELIHOOD CATEGORY IN TABLE A-7

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.

DETERMINATION OF FAILURE FREQUENCY INDEX NUMBERS IN TABLE A-8

Table A-8 is used to assign frequency index numbers to plant initiating events and control system failures as found in the columns of Table A-6. 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-6, accident sequence PPB2-1A involves loss of mass control over UO_2 in a blender. If criticality is the concern, failure does not occur unless UO_2 accumulates to a critical mass before the leak is stopped. For radiological consequences, any amount leaked may cause exposure. In assessing the frequency index, this factor should be considered because many control failures do not cause safety limits to be exceeded.

Table A-8 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 the applicant plant or in a comparable process elsewhere. Justification for specific assignments may be noted in the Comments column of Table A-6.

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.

DETERMINATION OF FAILURE PROBABILITY INDEX NUMBERS IN TABLE A-9

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 it is necessary then to 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-8. The probability of failure on demand may be the likelihood that it is in a failed state when demanded (availability), or that it fails to remain functional for a sufficient time to complete its mission.

DETERMINING MANAGEMENT MEASURES FOR SAFETY CONTROLS

Table A-12 is an acceptable way of listing those IROFS in all the accident sequences leading to consequences exceeding those identified in 70.61. The items listed should include all safety controls and all external events whose low likelihood is relied upon to meet the performance requirements of 10 CFR 70.61. Staff reviews this list to determine whether measures have been applied to each safety control adequate to assure their continual availability and reliability in conformance to 10 CFR 70.62(d). The types of management measures include maintenance, training, configuration management, audits and assessments, quality assurance, etc. Certain criteria for management measures are indicated in the Baseline Design Criteria; others are described in greater detail in Chapters 4 through 7 and Chapter 11. IROFS meeting all the provisions of these chapters have acceptable management measures. IROFS may, with justification, have lesser management measures than those described. However, every 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-6 and A-12 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 quality assurance 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 “uncontrolled” risk index shown in Table 6 of Appendix A to this Chapter, and (2) the accident likelihood index, “T”, also described in Table 6. In summary, items relied on to prevent or mitigate accidents which would

have unmitigated consequences in the two highest categories identified in 70.61 should satisfy the Baseline Design Requirements of 70.64 that apply.

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

IROFS must have satisfied all applicable Baseline Design Requirements of Section 70.64.

2. For those sequences that are initially evaluated as being in an acceptable risk category (an "uncontrolled" risk index of less than or equal to 4), a more detailed discussion is necessary. Some such accidents could have a relatively high uncontrolled likelihood (see discussion under 2.B below), yet be of low consequence such that the risk is acceptable without controls. However, if the accident consequence of interest is a nuclear criticality, 70.61(d) requires that this consequence be limited in likelihood to "highly unlikely", irrespective of the expected magnitude of consequence. Further, for accident sequences resulting in nuclear criticality, double contingency should be achieved, thus requiring at least one more item relied on for safety, typically a control, in addition to the initiating event. This control must have satisfied all applicable Baseline Design Requirements of Section 70.64. With this exception for criticality sequences, the following three cases apply:

2A. If the initiating event is <u>not</u> a control failure, then assurances for IROFS are not necessary. No additional risk reduction is required. However, for sequences claimed to be highly unlikely, the assessment that the initiating event has such a low frequency must be adequately justified in the application.

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

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

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

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

RISK-INFORMED REVIEW OF IROFS

NRC staff will review the IROFS failures and external events listed in Table A-12 in a risk-informed manner. Accident sequences having potential for higher risk will be subject to a more detailed review by staff to assure their adequacy.

The final results column of Table A-6 gives the risk indices for each accident sequence that was identified in the ISA. There are two indices, uncontrolled and controlled. The controlled index is a measure of risk without credit for the safety controls. If the uncontrolled risk index is a 6 or 9, while the controlled index is an acceptable value (less than 5), the set of safety controls involved are significant in achieving acceptable risk. That is, these controls have high risk significance. The uncontrolled 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.