

### 3. INTEGRATED SAFETY ANALYSIS AND INTEGRATED SAFETY ANALYSIS SUMMARY

#### 3.1 Purpose of Review

An integrated safety analysis (ISA) identifies potential accident sequences in the facility's operations, designates items relied on for safety (IROFS) to either prevent such accidents or mitigate their consequences to an acceptable level, and describes management measures to provide reasonable assurance of the availability and reliability of IROFS. Applicants for new licenses and persons holding licenses under Title 10, Part 70, "Domestic Licensing of Special Nuclear Material," of the *Code of Federal Regulations* (10 CFR Part 70) on September 18, 2000, must perform an ISA and submit a summary (referred to as an "ISA Summary") to the U.S. Nuclear Regulatory Commission (NRC) for approval. The ISA focuses on higher risk accident sequences with consequences that could exceed the criteria of 10 CFR 70.61, "Performance Requirements." The ISA Summary is a synopsis of the results of the ISA and contains information specified in 10 CFR 70.65(b).

The ISA and supporting documentation (such as piping and instrumentation diagrams, criticality safety analyses, dose calculations, process safety information, and ISA worksheets) would be maintained on-site at an existing facility. For an applicant seeking a license before commencing construction of a facility, full details concerning hardware, procedures, and programs usually would not exist. However, at the time of the operational readiness review<sup>1</sup> for a new facility, or major modifications to an existing facility, such details must exist to comply with the safety program requirements of 10 CFR 70 Subpart H, "Additional Requirements for Certain Licensees Authorized to Possess a Critical Mass of Special Nuclear Material." The level of detail that is acceptable in a license application and ISA Summary does not differ between existing and new facilities.

The NRC determines the acceptability of the applicant's ISA by reviewing a portion of the ISA documentation and any supporting documentation maintained onsite and by reviewing and approving the applicant's ISA Summary which, although not part of the license application, is placed on the public docket. Neither the ISA nor the ISA Summary is incorporated as part of the license.

Reviewers must confirm that an ISA Summary meets the regulatory requirements of 10 CFR 70.65, "Additional Content of Applications," and, specifically, that suitable IROFS and management measures have been designated for high-risk accident sequences and that programmatic commitments to maintain the ISA and ISA Summary are acceptable. The term "programmatic" is used here to refer to the organization, criteria, methods, and practices for conducting activities important to safety; such as the ISA program, criticality and other safety discipline programs, and the management measures programs addressed in Chapter 11. In fact, the primary purpose of the review conducted under the guidance of this chapter is to attain reasonable assurance that the applicant has established an ISA *program* that is, and will continue to be, in compliance with 10 CFR Part 70, Subpart H. Other chapters of this Standard Review Plan (SRP) offer guidance for review of management measures and other safety programs. This reasonable assurance of ISA program compliance is attained in part by a selective review of some of the ISA results, as described in Section 3.5 of this chapter under the subjects of

---

<sup>1</sup> The operational readiness review is an assessment review inspection performed by a multi-disciplinary inspection team to ensure that a plutonium or enrichment facility has been completed in accordance with the application or license, and so can be operated safely within the intended safety basis. For new facilities other than plutonium or enrichment facilities regulated under 10 CFR 70 Subpart H, or major modifications to existing ones, such ORRs, though not strictly required, are normally conducted.

'horizontal slice' and 'vertical slice' reviews. However, it is not normally necessary to review the full details of all processes and IROFS be reviewed in order to attain such reasonable assurance. An applicant may submit, for NRC approval, one ISA Summary for the entire facility, or multiple ISA summaries for individual processes (or groups of processes) in the facility as they are completed. Reviewers of ISA summaries for new and existing facilities may find it useful to examine the ISA and its supporting documentation to confirm the underpinnings of calculations, conclusions, and components of safety programs.

This chapter provides guidance for the NRC's review of two types of information submitted by applicants:

- (1) commitments regarding the applicant's safety program including the ISA, pursuant to the requirements of 10 CFR 70.62, "Safety Program and Integrated Safety Analysis"
- (2) ISA summaries submitted in accordance with 10 CFR 70.62(c)(3)(ii) and 10 CFR 70.65

In the case of license applications (either initial or renewal), applicants would submit both types of information. In the case of a license amendment, an applicant may submit either or both types of information, as needed, to address the areas amended.

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 10 CFR 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 facility (e.g., explosions, spills, and fires); and credible external events that could result in facility-induced consequences to workers, the public, or the environment, that could exceed the performance requirements of 10 CFR 70.61. As a minimum, external events normally include the following:
  - a. natural phenomena events such as floods, high winds, tornadoes, and earthquakes
  - b. fires external to the facility
  - c. transportation accidents and accidents at nearby industrial facilities
- (3) Designated engineered and administrative IROFS, and correctly evaluated the set of IROFS addressing each accident sequence, as providing reasonable assurance, through preventive or mitigative measures, and through application of supporting management measures (discussed in Chapter 11) that the performance requirements of 10 CFR 70.61 are met.

### **3.2 Responsibility for Review**

Primary: Assigned Licensing Reviewer

Secondary: Technical Specialists in Specific Areas

Supporting: Fuel Facility Inspectors

### 3.3 Areas of Review

This chapter addresses two types of submittals, including: (1) those containing descriptive commitments regarding the safety program, including 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 altered processes requiring revision of the ISA.

The safety program and ISA commitments and descriptions to be reviewed consist of: (1) process safety information (10 CFR 70.62(b)), (2) methods used to perform the ISA, (3) qualifications of the team performing the ISA (10 CFR 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 (10 CFR 70.62(d)). Documentation of these commitments and descriptions, as appropriate, will primarily appear within an ISA chapter in the license application. However, pursuant to Chapter 11 of this SRP, a separate chapter of an application may address the commitments to and descriptions of management measures.

An ISA Summary presents the results of ISA analyses performed for compliance with Subpart H of 10 CFR Part 70. 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 staff will review the ISA Summary submitted to the NRC, and the portions of the ISA and ISA documentation maintained on site to determine the adequacy of the applicant's ISA. The contents of the ISA Summary are specified in 10 CFR 70.65, include the following nine topics:

- (1) general description of the site
- (2) general description of the facility
- (3) description of facility processes, hazards, and types of accident sequences
- (4) demonstration of compliance with 10 CFR 70.61 performance requirements
- (5) description of the ISA team qualifications and ISA methods
- (6) descriptive list of IROFS
- (7) description of acute chemical exposure standards used
- (8) descriptive list of sole IROFS
- (9) definition of the terms "credible," "unlikely," and "highly unlikely"

The documentation supporting the ISA (e.g., piping and instrumentation drawings, engineered IROFS boundary descriptions, criticality safety analyses, dose calculations, process hazards analysis, process safety information, ISA worksheets, etc.) will normally be maintained at the facility site. It may be efficient for the reviewer to consult the ISA 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 could confirm that ~~low-risk~~ accident sequences that were not reported in the ISA Summary **because they were not credible** were correctly identified and analyzed in the ISA.

### 3.3.1 Safety Program and ISA Commitments

The NRC reviews the application to determine whether the applicant's commitments to establish a safety program and to perform and maintain an ISA are adequate. In the following, the phrase "process node" or "process" refers 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 ISA commitments 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") for those individuals who will conduct and maintain the ISA and ISA Summary.
- (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 method 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 determining 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 following applicant procedures:
  - a. performance of, and updates to, the ISA
  - b. review responsibility
  - c. ISA documentation
  - d. reporting of ISA Summary changes per 10 CFR 70.72(d)(1) and (3)
  - e. maintenance of ISA records per 10 CFR 70.62(a)(2)

### 3.3.2 ISA Summary and ISA Documentation

The NRC reviews the ISA Summary and, if necessary, the ISA and supporting ISA documentation to determine whether there is reasonable assurance that the applicant has performed a systematic evaluation of the hazards and has identified credible accident sequences,

IROFS, and management measures that satisfy the performance requirements of 10 CFR 70.61. The NRC confirms that credible 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 that exceeds the exposure limits stated in 10 CFR 70.61, are “highly unlikely” or “unlikely,” as appropriate. In addition, the NRC reviews accidents involving hazardous chemicals produced from licensed 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 (see SRP Chapter 6, “Chemical Process Safety”). On the other hand, accident sequences having unmitigated consequences that will not exceed the performance requirements of 10 CFR 70.61(c), once identified as such, do not require reporting in the ISA Summary.

The areas of review for the ISA Summary are as follows:

- (1) **Site:** The site description in the ISA Summary (see Section 1.3, “Site Description”) focuses on 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 focuses on 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, Hazards and Accident Sequences:** The process description in the ISA Summary addresses each process that was 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. This description must also include a list of the hazards (and interactions of hazards) for each process and the accident sequences that could result from such hazards and for which unmitigated consequences could exceed the performance requirements of 10 CFR 70.61.
- (4) **Demonstration of Compliance with 10 CFR 70.61:** For each applicable process, this section presents the following information that should be developed in the ISA to demonstrate compliance with the performance criteria of 10 CFR 70.61:
  - a. postulated consequences and comparison to the consequence levels identified in 10 CFR 70.61, as well as information, such as inventory and release path factors supporting the results of the consequence evaluation
  - b. information showing how the applicant established the likelihoods of accident sequences that could exceed the performance requirements of 10 CFR 70.61
  - c. information describing how designated IROFS protect against accident sequences that could exceed the performance requirements of 10 CFR 70.61
  - d. information on management measures applied to the IROFS (addressed in greater detail in Chapter 11)

- e. information on how the criticality monitoring requirements of 10 CFR 70.24, "Criticality Accident Requirements," are met
  - f. if applicable, ways that the baseline design criteria of 10 CFR 70.64, "Requirements for New Facilities or New Processes at Existing Facilities," are addressed
- (5) Team Qualifications and ISA Methods: This section should discuss the applicant's ISA team qualifications and ISA methods, as described 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. Specific examples of the application of ISA methods should be included in the ISA Summary to enable the reviewer to understand their selection and use.)
  - (6) List of IROFS: This list describes the IROFS for all intermediate- and high-consequence accidents in sufficient detail to permit an understanding of their safety function.
  - (7) Chemical Consequence Standards: This discussion identifies the applicant's quantitative standards for assessing the chemical consequence levels specified in 10 CFR 70.61, as described in the ISA Summary.
  - (8) List of Sole IROFS: This list identifies those IROFS that are the sole item preventing or mitigating an accident for which the consequences could exceed the performance requirements of 10 CFR 70.61.
  - (9) Definitions of "Unlikely", "Highly Unlikely" and "Credible": The applicant must define the terms "unlikely," "highly unlikely," and "credible," as used in the ISA Summary.

The regulations in 10 CFR 70.65(b) list the types of information required to be submitted in an ISA Summary. This includes generic information, such as site description, ISA methods, and ISA team qualifications. This also includes process-specific information, such as a list of IROFS, general descriptions of types of accidents sequences, and "information demonstrating compliance with 10 CFR 70.61." To meet the latter requirement, an applicant would have to provide, at a minimum, likelihood and consequence information for each type of process accident sequence identified in the ISA Summary. To evaluate the effectiveness of the applicant's likelihood and consequence evaluation methods, the reviewer should also examine the analyses of some accident sequences that are not reported in the ISA Summary for which the applicant established that consequences will not to exceed the performance requirements of 10 CFR 70.61.

In some simple cases, the information normally contained in the ISA Summary process descriptions and list of IROFS might be sufficient to enable the reviewer to understand how compliance is achieved when taken together with the description of ISA likelihood evaluation methods and criteria. However, in general, the applicant should describe how its ISA team evaluated a credible accident likelihood to be "highly unlikely" or "unlikely".

The reviewer should evaluate the efficacy of the applicant's ISA methods. To do this, in addition to reviewing the description of the ISA methods, the reviewer will need to understand how these methods have been applied in practice to the wide diversity of process safety designs in the facility. Examples included in the ISA Summary of how the methods are applied to a representative sample of processes would help the reviewer to understand the applicant's ISA methods. However, if such examples providing details of how the methods were applied are not provided in the ISA Summary, such information may be available at the applicant's site, as part of the overall safety information records.

The NRC review of the applicant's example accident sequence evaluations included in the ISA Summary is not a substitute for the "vertical slice" and "horizontal" reviews that should be performed using detailed information at the site. This onsite evaluation of ISA documentation and processes must be selected by the NRC to confirm that the ISA was actually performed as described in the ISA Summary.

### 3.4 Acceptance Criteria

#### 3.4.1 Regulatory Requirements

The regulation in 10 CFR 70.62 specifies the requirement to establish and maintain a safety program, including performance of an ISA. Paragraph (c) of 10 CFR 70.62 specifies requirements for conducting an ISA, which include a demonstration that credible high-consequence and intermediate-consequence events meet the safety performance requirements of 10 CFR 70.61. The requirement to prepare and submit an ISA Summary for NRC approval, stated in 10 CFR 70.65(b), also describes the contents of an ISA Summary. The regulation in 10 CFR 70.72, "Facility Changes and Change Process," sets forth requirements for maintaining a current ISA, ~~ISA documentation, and ISA Summary and other safety program documentation~~ when changes are made to the site, structures, processes, systems, equipment, components, computer programs, and activities of personnel; ~~however, the ISA Summary need only be updated annually.~~

The information to be included in the ISA Summary can be divided into four categories including (1) site and facility characteristics, (2) ISA methods, (3) hazards and accident analysis and (4) IROFS. Table 3.1 summarizes the information requirements of each category, the corresponding regulatory citation, and the section of this chapter that describes the expectations for such information.

**Table 3.1 Information Requirements for the ISA Summary**

Information Category and Requirement	10 CFR Part 70 Regulatory Citation	NUREG-1520, Chapter 3 Section Reference
<b><u>Site and Facility Characteristics:</u></b> Site description	70.65(b)(1)	3.4.3.2(1)
Facility description	70.65(b)(2)	3.4.3.2(2)
Criticality monitoring and alarms	70.65(b)(4)	3.4.3.2(4c)
Compliance with baseline design criteria, criticality monitoring, and alarms	70.64 (if applicable) 70.65(b)(4)	3.4.3.2(4d)
<b>ISA Methods</b>		
ISA method(s) description	70.65(b)(5)	3.4.3.2(5)
ISA team description	70.65(b)(5)	3.4.3.2(5)
Quantitative standards for acute chemical exposures	70.65(b)(7)	3.4.3.2(7)
Definition of "unlikely," "highly unlikely," and "credible"	70.65(b)(9)	3.4.3.2(9)
<b>Hazards and Accident Analysis</b>		
Description of processes analyzed	70.65(b)(3)	3.4.3.2(3a)
Identification of hazards	70.65(b)(3)	3.4.3.2(3b)
Description of accident sequences	70.65(b)(3)	3.4.3.2(3c)
Characterization of high- and intermediate-consequence accident sequences	70.65(b)(3)	3.4.3.2(3c)
<b>Items Relied on for Safety</b>		
List and description of items relied on for safety (IROFS)	70.65(b)(6)	3.4.3.2(6)
Description of IROFS' link to accident sequences to show 10 CFR 70.61 compliance	70.65(b)(6)	3.4.3.2(4) and (6)
IROFS management measures	70.65(b)(4)	3.4.3.2(4b) and (6)
List of sole IROFS	70.65(b)(8)	3.4.3.2(8)

### 3.4.2 Regulatory Guidance

NUREG-1513, "Integrated Safety Analysis Guidance Document," issued May 2001, contains guidance applicable to performing an ISA and documenting the results. NUREG/CR-6410, "Nuclear Fuel Cycle Facility Accident Analysis Handbook," issued March 1998, provides guidance on acceptable methods for evaluating the chemical and radiological consequences of potential accidents. NUREG-1601, "Chemical Process Safety at Fuel Cycle Facilities," issued August

1997, provides guidance on chemical safety practices acceptable for compliance with the regulations.

### 3.4.3 Regulatory Acceptance Criteria

The acceptance criteria for an ISA are derived from and support compliance with the relevant requirements of 10 CFR Part 70. 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 the performance requirements of 10 CFR 70.61. Some of the acceptance criteria address the programmatic commitments made by the applicant 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 ensure that the relevant accident sequences will meet the performance requirements of 10 CFR 70.61. The acceptance criteria are thus intended to support the ultimate finding of the license review that based on the information submitted and reviewed, there is reasonable assurance that the proposed facility, IROFS, safety programs, and management measures conforming to the commitments in the application are in compliance with the regulations, and provide adequate protection of public health and safety.

A high level of detail describing the process designs and IROFS might not be submitted with the license application or ISA Summary. In other words, the applicant might not provide information about all the components in a system, because not every component would be a safety-related component. In particular, for proposed new facilities, the level of detail may be limited since the hardware has not actually been fabricated. However, the applicant must describe the IROFS in enough detail to permit an understanding of the intended safety function; **and to permit an assessment that it is capable of the reliability relied upon utilized in the evaluation of likelihoods of accident sequences.** Additional details may be obtained for processes selected for the vertical slice review by visiting the applicant's site. While there may be an actual difference in level of detail that is known about processes and IROFS, as documented at the applicant's site, between existing and proposed new facilities. ~~However,~~ the minimum level of detail that is sufficient in descriptions of processes and IROFS, as documented in the ISA Summary, does not differ between existing and proposed new facilities.

The purpose of the review, and its acceptance criteria, for most facilities, is primarily to permit a finding that the applicant's safety program, including the ISA program as described, provide reasonable assurance that compliance will be achieved. However, to generate the ISA Summary, which is a required submission, the applicant must first perform an ISA. This in turn requires that the applicant identify process designs, accident sequences, and IROFS. These latter items are not programmatic, but are elements of design and analysis of design. Attainment of reasonable assurance that the ISA program is and will be effective does not usually require that all safety elements and IROFS be reviewed in full detail, nor is it required that the applicant's description of IROFS and process designs be at the level of detail that will eventually exist at the time of operations (see the discussion of vertical slice review in Section 3.5). The requisite level of detail to achieve reasonable assurance may vary among processes depending on factors such as: use of established technology, commitment to standards, applicant expertise, industry experience, safety margins, and inherent difficulty in achieving the safety function. However, the underlying requirements for the descriptions are exactly the same for each process and IROFS; namely: "...a description of each process...in sufficient detail to understand the theory of operation..." [70.65(3)]; and: "a description of IROFS...in sufficient detail to understand their functions in relation to the performance requirements..." [70.65(8)]. Thus there is no different requirement for new technology vs. old, but more explanatory detail may be necessary to meet the above requirements on "needed to understand".

#### 3.4.3.1 Safety Program and ISA Commitments

This section discusses the acceptance criteria for license commitments pertaining to the facility's safety program including the performance of an ISA. A number of specific safety program requirements related to the ISA appear in 10 CFR Part 70. Section 3.4.3.2 presents the acceptance criteria for the content of the ISA Summary. These include the primary requirements that an ISA be conducted, and that, based on the ISA Summary submitted, there is reasonable assurance that the applicant's facility and safety program complies with the ISA requirements of 10 CFR Part 70 Subpart H, including the performance requirements of 10 CFR 70.61. For each component of the safety program, several elements may be necessary, including organization, assignment of responsibilities, management policies, required activities, written procedures for activities, use of industry consensus standards, and technical safety practices, among others.

Procedures and industry standards for hardware safety controls vary according to the type of equipment, and by the degree of reliability and performance required in -specific applications. For this reason, blanket commitments to apply all standards in all cases may not appear in the license application. However, some standards on engineering practices and hardware and software design or analysis are generic. Hence, an applicant may specify a general commitment to such a generic standard; or may make conditional commitments to standards, subject to specified applicability criteria. The purpose of such commitments is to support likelihood or other performance evaluations for compliance with the regulations. Some standards have been endorsed, possibly with exceptions,- in NRC guidance. Such commitments to standards are acceptable if they are consistent with their use in demonstrating compliance, and with specific NRC guidance.

Among those engineering practices and standards that are generically applicable to IROFS and safety controls are those that apply to personnel activities that are relevant to administrative controls, management measures, or human-machine interfaces. This area is called human factors engineering. Thus human factors engineering should generally be part of the safety program. Human factors practices should be incorporated into the applicant's safety program sufficiently to assure that IROFS and management measures perform their functions in meeting the requirements of 10 CFR 70. Appendix E of this chapter describes areas of review and acceptance criteria for human factors engineering in the context of 10 CFR 70 for fuel cycle facilities.

The applicant's commitments for each of the three elements of the safety program defined in 10 CFR 70.62(a) should be acceptable if they comply with the following:

- (1) Process Safety Information
  - a. 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 should include information pertaining to the following:
    - i. The description of hazards of all materials used or produced in the process, which should include 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)].

- ii. The discussion of the technology of the process 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, and concentration), and evaluation of the health and safety consequences of process deviations.
- iii. The description of the equipment used in the process should include general information on topics such as the materials of construction, piping and instrumentation diagrams (P&IDs), ventilation; design codes and standards employed, material and energy balances, IROFS (e.g., interlocks, detection, or suppression systems), electrical classification, and relief system design and design basis.

- b. The applicant includes procedures and criteria for changing the ISA along with a commitment to designing and implementing 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, as well as procedures and responsibilities for updating the facility's ISA.
- c. The applicant commits to engaging personnel with appropriate experience and expertise in engineering and process operations to maintain the ISA. The ISA team for a process should consist of individuals who are knowledgeable in the facility's ISA methods and the operation, hazards, and safety design criteria of the particular process.

(2) ISA

- a. The applicant has conducted and commits to continuing to maintain an ISA of appropriate complexity for each process, such that it identifies (i) radiological hazards, (ii) chemical hazards that could increase radiological risk, (iii) facility hazards that could increase radiological risk, (iv) potential accident sequences, (v) consequences and likelihood of each accident sequence, and (vi) IROFS including the assumptions and conditions under which they support compliance with the performance requirements of 10 CFR 70.61. 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 Section 3.4.3.2 of this SRP, and Appendix A to this chapter.
- b. The applicant commits to maintaining the ISA and its supporting documentation so that it is accurate and up-to-date by means of a suitable configuration management system and to submitting changes in the ISA Summary, to the NRC, in accordance with 10 CFR 70.72(d)(1) and (3). The ISA must account for any changes made to the facility or its processes (e.g., changes to the site, operating procedures, or 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 methods. For any revisions to the ISA, the applicant commits to using personnel

with qualifications similar to those of ISA team members who conducted the original ISA.

- c. The applicant commits to training personnel in the facility's ISA methods and/or using suitably qualified personnel to update and maintain the ISA and ISA Summary.
- d. The applicant commits to evaluating proposed changes to the facility or its operations by means of the ISA methods and to designating new or additional IROFS and appropriate management measures as required. The applicant also agrees to promptly evaluate the adequacy of existing IROFS and associated management measures and to make any required changes that may be affected by changes to the facility and/or its processes. If a proposed change results in a ~~revised accident sequence in the ISA Summary~~ **new type of accident sequence (e.g., different initiating event, significant changes in the consequences)** or increases the consequences and/or likelihood 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.
- e. The applicant commits to addressing any unacceptable performance deficiencies in the IROFS that are identified through updates to the ISA.
- f. The applicant commits to maintaining written procedures on site.
- g. The applicant commits to establishing all IROFS (if not already established) and to maintaining them so that they are available and reliable when needed.

In citing industry consensus standards, the applicant should delineate specific commitments in the standards that will be adopted. The applicant should provide justification if not all of the required elements of a standard are adopted.

### (3) Management Measures

The applicant commits to establishing management measures (which are evaluated using SRP Chapter 11) that constitute the principal mechanism for ensuring the reliability and availability of each IROFS.

#### 3.4.3.2 ISA Summary and ISA Documentation

Information in the ISA Summary should provide the basis for the reviewer to conclude that there is reasonable assurance that the identified IROFS will satisfy the performance requirements of 10 CFR 70.61. To do this, the reviewer must conclude that the applicant's ISA program has the capability to identify appropriate IROFS, and that IROFS identified in the ISA Summary are adequate to control the potential accidents of concern at the facility. The accidents of concern are those for which the 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 so that the performance requirements of 10 CFR 70.61 can be met. To support such a review, the ISA Summary must include sufficient information about an accident sequence and the proposed IROFS to allow the reviewer to assess the contributions of the IROFS to prevention or mitigation. The ISA Summary must contain enough information concerning the ISA methods and the qualifications of the ISA team that performed the ISA and any other resources

employed to give the reviewer confidence that the potential accidents identified are reasonably complete.

In addition, the reviewer needs to determine that appropriate management measures will be in place to ensure the availability and reliability of the identified IROFS, when needed. Chapter 11 of this SRP addresses the review of designated management measures

The following acceptance criteria address each of the content elements of the ISA Summary required by 10 CFR 70.65(b). For new facilities, the reviewer should also evaluate those aspects of the design that address the baseline design criteria of 10 CFR 70.64 applicable to individual processes. Thus, the following nine content elements have defined acceptance criteria:

- (1) general description of the site
- (2) general description of the facility
- (3) description of facility processes, hazards, and types of accident sequences
- (4) demonstration of compliance with 10 CFR 70.61 performance requirements
- (5) description of the ISA team qualifications and ISA methods
- (6) descriptive list of IROFS
- (7) description of acute chemical exposure standards used
- (8) descriptive list of sole IROFS
- (9) definitions of "credible," "unlikely," and "highly unlikely"

Detailed acceptance criteria for each element of the ISA Summary follow:

(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, taking into account 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 the most 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 allow assessment of their impact on facility safety and to their likelihood of occurrence. At a minimum, the 100-year flood should be postulated, consistent with U.S. Army Corps of Engineers flood plain maps.

The applicant should also provide earthquake accelerations for the site associated with a 250-year and 500-year earthquake. The discussion should identify all design-basis natural events for the facility, indicates which events are considered incredible, and describes the basis for that determination. The assessment should also indicate 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 IROFS. 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 a minimum, the applicant should adequately identify and describe the following:

- 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. restricted area and controlled area boundaries.
- c. 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.
- d. the location and arrangement of buildings on the facility site.

## (3) Processes, Hazards, and Accident Sequences

### a. Processes

The descriptions of processes in the ISA Summary must include all processes in which upset conditions could credibly lead to accidents with high or intermediate consequences. No areas or processes can be omitted, unless screened out on the basis of non-credibility of accidents.

The description in the ISA Summary of the processes analyzed as part of the ISA [10 CFR 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 assess compliance with the performance requirements of 10 CFR 70.61. A description at a systems level is acceptable, provided that it permits the NRC reviewer to adequately evaluate (1) the completeness of the hazard and accident identification tasks and (2) the likelihood and consequences of the accidents identified. If the information is available elsewhere in the application and is adequate to support the purposes of the ISA Summary, reference to the appropriate sections is considered acceptable. The descriptions of processes must permit an understanding of how the set of IROFS in that process could reliably ~~prevent the process from exceeding safety limits~~ perform their safety function for each high and intermediate consequence accident sequence. Hence all process designs must be described in sufficient detail to reasonably permit identification of all accident sequences and IROFS to prevent or mitigate them.

The level of detail in process safety documentation held at the site would normally be greater than the descriptions in the ISA Summary; and may include some or all of the information listed as items ii through iv below as needed.

Formatted: Normal, Indent: Left: 0.23"

i. \_\_\_\_\_Basic process function and theory includes a general discussion of the basic theory of \_\_\_\_\_the process. Normally this would be expected to include:

- (1) Parameters to be controlled and strategy for complying with 10 CFR 70.61;
  - (2) Chemical or mechanical theory principles, materials, and quantities needed to understand the hazards and safety functions;
  - (3) Normal and potential transport and changes in materials in the process.
- ii. Major components include the general arrangement, function, and operation of major components in the process. If appropriate, it could also include arrangement drawings and process schematics showing the major components and instrumentation, and flow sheets showing compositions of the various process streams.
- iii. Process design and equipment include a discussion of process design, equipment, and instrumentation that is sufficiently detailed to permit an adequate understanding of the results of the ISA. As appropriate, 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, and other factors.
- iv. Process safety limits and margins on variables (e.g., temperatures, pressures, flows, fissile mass, enrichment, and composition) that are controlled by IROFS to ensure safe operations of the process, should be specified, because these limits and margins would thus be needed to understand the likelihood of failure assigned by the applicant to the IROFS. For example, if a process is designed, and an IROFS procedure specified, to ensure critical mass control by double-batching proof, the margin from a single batch to the subcritical limit should be specified. Traditionally the single batch is 45 percent of the subcritical limit.

b. Hazards

The description of process hazards provided in the ISA Summary is acceptable if it identifies, for each process, all types of hazards that are relevant to determining compliance with the performance criteria of 10 CFR 70.61. That is, the acceptance criterion is completeness. All hazards that could result in an accident sequence in which the consequences could exceed the performance requirements of 10 CFR 70.61 should be listed, even if later analysis of a particular hazard shows that resulting accident sequences do not exceed these limits. Otherwise the reviewer cannot determine completeness. General exclusion from 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 performance requirements of 10 CFR 70.61 cannot be exceeded. In this case, the bounding inventories or conditions, if under the control of the applicant, become IROFS.

Any locations where hazardous regulated material, including fissile material, could ~~ever~~ **accidentally** be located, ~~even if only by accident~~, should **also** be considered. Improperly screening out locations and processes that are not normally hazardous, but that could

become so in upset conditions, can lead to a failure to apply IROFS to prevent such upsets; and potential accidents arising from them.

The list of process hazards is acceptable if the ISA Summary provides the following information:

- i. a list of materials (radioactive, fissile, flammable, and toxic) or conditions that could result in hazardous situations (e.g., loss of containment of licensed nuclear material), including the maximum intended inventory amounts and locations of the hazardous materials at the facility
- ii. potential interactions among materials or conditions that could result in hazardous situations
- c. Accident Sequences

The general description of types of accident sequences in the ISA Summary is acceptable if the reviewer can determine the following:

- i. The applicant has identified all **types of accidents** for which the consequences could exceed the performance requirements of 10 CFR 70.61. **The level of detail required in describing accidents is closely related to the level of detail in describing IROFS, as many events leading to consequences of concern in 10 CFR 70.61 are failures of IROFS. It is not usually necessary to specify all modes and mechanisms by which the IROFS failure could occur in order to understand the role that the IROFS plays in preventing or mitigating the accident.**
- ii. The applicant has identified how the IROFS listed in the ISA Summary protect against each such type of accident.

To satisfy the requirement that all accidents be identified, the applicant must describe the process design in sufficient detail. In particular, all IROFS need to be specified. The level of detail in specifying the process and IROFS must be sufficient to permit a reasonable understanding as to how the safety function will be performed so as to meet the performance requirements of section 70.61.

General types of accident sequences differ if they consist of a different set of IROFS failures. Thus, several processes, each using a set of IROFS that is functionally of the same type (e.g., having the same mechanical, physical, and/or electrical principle of operation), can be summarized as a single type of accident sequence 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 generally acceptable as a description of an accident to merely list the type of hazard, or the controlled parameters, without referencing the items relied on to control the parameters or hazard. The description of general types of accident sequences is acceptable if it covers all types of sequences, initiating events, and IROFS failures. **Initiating events may be either a failure of an IROFS or an external event.** Initiating events can be (1) an external event such as a hurricane or earthquake, (2) a facility event external to the process being analyzed (e.g., fires, explosions, failures of other equipment, flooding from facility water sources), (3) deviations from normal operations of the process (credible abnormal events), or (4) failures of an IROFS in the process. Human errors that are initiating events would generally be administrative IROFS failures. The description of a general type of accident sequence is acceptable if it permits

the reviewer to determine how each accident sequence for which the consequences could exceed the performance requirements of 10 CFR 70.61 is protected against by IROFS or a system of IROFS.

One acceptable way to do this is to show a fault tree on which the basic events are IROFS failures. Another acceptable way is to provide a table in which each row displays the events in an accident sequence, such as in Appendix A, Table A-7, where, in general, each event is a failure of an IROFS. Another acceptable way is to provide a narrative summary for each process describing the sequence of events in each type of accident.

To demonstrate completeness, the ~~description of Process Hazard Analysis identifying~~ general types of accident sequences must ~~be~~ use systematic methods and consistent references. Therefore, each description of a general type of accident sequence is acceptable if it meets the following criteria:

- i. An acceptable method of hazard identification and process hazard analysis is used in accordance with the criteria of NUREG-1513.
- ii. The selected method is correctly applied.
- iii. The applicant does not overlook any **type of** accident sequence for which the consequences could exceed the performance requirements of 10 CFR 70.61. **A key test of whether a type of accident has been 'overlooked' is whether IROFS have been identified to meet the performance requirements.**
- iv. The applicant uses a method of identifying facility processes that ensures identification of all processes.

During the early phases of an ISA, accidents will be identified for which the consequences may initially be unknown. These accidents will later be analyzed and may be shown to have consequences that are less than the levels identified in 10 CFR 70.61.

The ISA Summary need not list as a separate type of accident sequence, every conceivable permutation of an accident. Accidents having characteristics that all fall in the same categories can be grouped as a single type of accident in the ISA Summary provided that the following conditions are fulfilled:

- i. The initiating IROFS failures or events have the same effect on the system.
- ii. They all consist of failures of the same IROFS or system of IROFS.
- iii. They all result in violation of the safety limit on the same parameter.
- iv. They all result in the same type and severity categories of consequences.

#### (4) Information Demonstrating Compliance with the Performance Requirements of 10 CFR 70.61

##### a. Accident Sequence Evaluation and IROFS Designation

The regulation in 10 CFR 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 ISA Summary should provide sufficient information to demonstrate the following

- i. Credible high-consequence events are highly unlikely.
- ii. Credible intermediate-consequence events are unlikely.
- iii. Under normal and credible abnormal conditions, all nuclear processes are subcritical.

The performance requirements of 10 CFR 70.61 have three elements, including completeness, consequences, and likelihood.

Completeness refers to the fact that the ISA must address *each* credible event. Consequence refers to the magnitude of the chemical and radiological doses of the accident and is the basis for classification of an accident in 10 CFR 70.61 to be a high or intermediate consequence event. 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 also show the basis for and 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, fault trees, or tabular summaries. Appendix A to this chapter shows one example of how an application can present this information.

Each of these performance requirements (completeness, consequences, and likelihood) is discussed below.

- i. Completeness is demonstrated by correctly applying an appropriate accident identification method, as described in NUREG-1513, "Integrated Safety Analysis Guidance Document." Completeness can be effectively displayed by using an appropriate diagram or description of the identified accidents. Item (3) (above) covers specific acceptance criteria for completeness.
- ii. Consequence information in the ISA Summary is acceptable for showing compliance with 10 CFR 70.61 provided that the following conditions are met.
  - For each accident for which the consequences could exceed the performance requirements of 10 CFR 70.61, the ISA Summary 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 ISA Summary that applies to or bounds that accident.
  - The consequences were calculated using a method and data consistent with NUREG/CR-6410, or another method described and justified in the methods description section of the ISA Summary.

- All consequences that could result from the accident sequence have been evaluated. That is, if an accident can result in a range of consequences, all possibilities must be considered, including the maximum source term and most adverse weather that could occur. In other words, due to possible variations in weather, or other conditions, the consequences of a type of potential accident may vary. If, for some such conditions, the consequences will be high, then the subset of such accidents thus resulting in high consequences are a “high consequence accident sequence” in the ISA; even though for average conditions such high consequences would not result. If such conditions are *unlikely* to occur, credit can be taken for this in the evaluation of likelihood.
- The ISA Summary correctly assigns each type of accident to one of the consequence categories of 10 CFR 70.61 (namely, high, or intermediate).

Unshielded nuclear criticality accidents are considered to be high consequence events, because the radiation exposure that an individual could receive exceeds the acute 1 sievert (Sv ) (100 rem) dose established by 10 CFR 70.61(b)(1). For processes with effective engineered shielding, criticalities may actually produce doses below the intermediate consequences of 10 CFR 70.61. As stated in 10 CFR 70.61(d), such processes must, nevertheless be subcritical for all **normal and** credible abnormal conditions, and primary reliance must be on prevention. This applies, notwithstanding shielding or other mitigative features. If needed, NUREG/CR-6410 provides methods for estimating the magnitudes of criticality events that can be applied for workers or members of the public at varying distances from the event.

iii. Likelihood information in the ISA Summary is acceptable to show compliance with 10 CFR 70.61, provided that the following conditions are met:

- The ISA Summary specifies the likelihood of each general type of accident sequence that could exceed the performance requirements of 10 CFR 70.61.
- The likelihoods are derived using an acceptable method described in the ISA Summary’s methods section.
- The likelihoods comply with acceptable definitions of the terms “unlikely” and “highly unlikely,” as described in this SRP chapter. 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 violate the requirement, which is not the intent.

b. Management Measures

According to 10 CFR 70.65(b)(4), the application must describe the management measures to be applied to IROFS ~~for each accident sequence for which the consequences could exceed the performance requirements of 10 CFR 70.61 listed in the ISA Summary as required to meet the requirements of 10 CFR 70.61~~. Chapter 11 of this SRP provides detailed criteria for use in evaluating the adequacy of such management measures.

c. Criticality Monitoring

The regulation in 10 CFR 70.24 defines specific sensitivity and coverage requirements for criticality monitors. Acceptance criteria and review of information supporting a demonstration of compliance with 10 CFR 70.24 is found in Chapter 5 of this SRP.

10 CFR 70.24 also requires specific emergency preparations. Specifically, the application should provide information to demonstrate that the applicant's equipment and procedures are adequate to ensure that these requirements are met.

d. Requirements for New Facilities or New Processes at Existing Facilities

The baseline design criteria specified in 10 CFR 70.64 must be used, as applicable, for new facilities and new processes at existing facilities. If the application involves such new facilities or processes, the ISA Summary should explain how the design of the facility addresses each baseline design criterion. For deterministic design criteria such as double-contingency, the process-specific information may be provided, along with the other process information in the ISA Summary. The application should also describe the design-basis events and safety parameter limits. In addition, the application should provide methods, data, and results of analysis showing compliance with these design bases for individual processes and facilities.

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

(5) ISA Team Qualifications and ISA Methods

The ISA teams [10 CFR 70.62(c)(2)] and their qualifications as stated in the ISA Summary are acceptable if the following criteria are met:

- The ISA team has a leader who is formally trained and knowledgeable in the ISA methods 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.
- At least one member of the ISA team has thorough, specific, and detailed experience in the type of process design under evaluation.
- The team has a variety of process design and safety experience in the 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.
- A manager provides overall administrative and technical direction for the ISA.

The description of the ISA methods is acceptable if the following criteria are met:

- a. Hazard Identification Method. The hazard identification method selected is considered acceptable if it meets the following criteria:

- i. The description includes 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 should include maximum intended inventory amounts and the location of the hazardous materials at the facility.<sup>1</sup>
  - ii. The method has determined potential interactions between materials or upset conditions that could result in hazardous situations where not normally present.
- b. Process Hazard Analysis Method. The process hazard analysis method is acceptable if it involves selecting one of the methods described in NUREG-1513 in accordance with the selection criteria established in that document. Methods not described in NUREG-1513 may be acceptable provided that they fulfill the following conditions:
- i. Criteria are provided for their use for an individual process, and are consistent with the principles of the selection criteria in NUREG-1513.
  - ii. The method 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. The method provides reasonable assurance that the applicant can identify all significant accident sequences (including the IROFS used to prevent or mitigate the accidents) that could exceed the performance requirements of 10 CFR 70.61.<sup>2</sup>
  - iv. The method considers the interactions of identified hazards and proposed IROFS, including system interactions that could result in an accident sequence for which the consequences could exceed the performance requirements of 10 CFR 70.61.
  - v. The method addresses all modes of operation, including startup, normal operation, shutdown, and maintenance.
  - vi. The method addresses hazards resulting from process deviations (e.g., high temperature, and high pressure), initiating events internal to the facility (e.g., fires or explosions), and hazardous credible external events (e.g., floods, high winds, earthquakes, and 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. The method 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. The method adequately considers common mode failures and system interactions in evaluating systems that rely on redundant controls.

---

<sup>1</sup> At a minimum, the inventory list should include the following hazardous materials if present onsite: ammonia; fines (uranium oxide dust, beryllium); flammable liquids and gases; fluorine; hydrofluoric acid; hydrogen; nitric acid; organic solvents; propane; uranium hexafluoride; and Zircaloy.

<sup>2</sup> The release of hazardous chemicals is of regulatory concern to the NRC only to the extent that such hazardous releases result from the processing of licensed nuclear material or have the potential to adversely affect radiological safety.

- ix. The ISA Summary provides justification that the individual method would comply with conditions (ii) through (viii), above.
- c. Consequence Analysis Method. The methods used for ISA consequence evaluation, as described in the ISA Summary, are acceptable, provided that the following conditions are met:
  - i. The methods are consistent with the approaches described in NUREG/CR-6410.
  - ii. The use of generic assumptions and data is reasonably conservative for the types of accidents analyzed.
- d. Likelihood Evaluation Method. The method for evaluating the likelihood of accident sequences, as described in the ISA Summary, is considered acceptable, provided the following conditions are met:
  - i. The method clearly shows how each designated IROFS acts to prevent or mitigate the consequences (to an acceptable level) of the accident sequence being evaluated.
  - ii. When multiple IROFS are designated for an accident sequence, the method considers the interaction of all such IROFS, as in a logic diagram or tabulation that accounts for the impact of redundancy, independence, and surveillance 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. When applicable, such likelihood criteria should include the 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 safety grading (if any) of the management measures applied to the IROFS.
  - iv. The method evaluates the likelihood of each accident sequence as “unlikely”, “highly unlikely”, or neither, as defined by the applicant, in accordance with Section 3.4.3.2, item 9, of this chapter.
  - v. For nuclear criticality accident sequences, the method evaluates compliance with 10 CFR 70.61(d). That is, even in a facility with engineered shielding to limit the consequences of nuclear criticalities, *preventive* controls must be in place that are sufficient to ensure that the process is subcritical for all credible abnormal conditions. Compared to unshielded processes, a moderately higher likelihood may be permitted in preventing such events, consistent with ANSI/ANS Standard 8.10, “Criteria for Nuclear Criticality Safety Controls in Operations with Shielding and Confinement,” reaffirmed in 2005. In particular, criticality cannot result from any credible failure of a single IROFS. 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 must consider, and the ISA Summary must document, the actual magnitude of those margins when they are part of the reason that the postulated accident sequence resulting in criticality is deemed highly unlikely.

Appendix A to this chapter provides an example of one acceptable method for evaluating likelihood that is based on a likelihood index. Appendix B offers additional guidance on

acceptable methods for qualitative evaluation of likelihood. Appendix C discusses issues relating to the use of initiating event frequencies in demonstrating compliance with the likelihood requirements. Appendix D discusses acceptable ways for the ISA to address natural phenomena.

#### (6) Descriptive List of All IROFS

The "list describing items relied on for safety" required by 10 CFR 70.62(c)(1)(vi) is acceptable, provided that the following conditions are met:

a The list includes *all* IROFS in the identified high and intermediate consequence accident sequences.

b The *description* of the IROFS *may* includes management measures applied to the IROFS (including the safety grading); *should include* the characteristics of its preventive, mitigative, or other safety function; *and may include* assumptions and conditions, such as safety limits or margins, *if these are needed to understand how the item is capable of achieving compliance with 10 CFR 70 Subpart H. under which the item is relied on to support compliance with the performance requirements of 10 CFR 70.61.*

The above acceptance criteria are explained in greater detail below.

- a. The primary function of the list describing each IROFS is to document the safety basis of all processes in the facility. This list assists in ensuring that the items (IROFS) are not degraded without a justifying safety review. Thus, the key feature of this list is that it includes *all* IROFS. To be acceptable, no item, *aspect, feature, or property control, or control system* of a process that is needed to show compliance with the safety performance requirements of the regulation may be omitted from this list [see 10 CFR 70.61(e)]. *However, sets of hardware or procedures that perform the same safety function may be referred to as a single set of IROFS, and do not need to be individually identified.* The list of IROFS may *erroneously* be incomplete in a number of ways: (1) an ineffective method of identifying accident sequences may have been used, (2) in applying the method to identify accidents something was overlooked, (3) a whole area or process subject to accidents was improperly screened out, or simply omitted from the ISA, (4) IROFS were not applied to an identified accident, or (5) the list of accidents was incomplete because of incompleteness in the process design itself. *The reviewer should attempt, in the horizontal slice review, to determine if any of these errors has occurred.*
- b. 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. The ISA Summary need not provide a breakdown of hardware IROFS by component or identify all support systems. However, the ISA documentation maintained onsite, such as system schematics and/or descriptive lists, should contain sufficient detail about items within a hardware IROFS, such that it is clear to the reviewer and the applicant, what structure, system, equipment, or component is included within the hardware IROFS' boundary and would, therefore, be subject to management measures specified by the applicant. Some examples of items within a hardware IROFS are detectors, sensors, electronics, cables, valves, piping, tanks, dykes, etc. In addition, ISA documentation should

Formatted: Indent: Left: 0", Tab stops: Not at 1.06"

also identify essential utilities and support systems on which the IROFS depends to perform its intended function. Some examples of these are backup batteries, air supply, steam supply, etc. 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.

- c. The essential features of each IROFS 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 may need to 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 IROFS should identify its expected function, conditions needed for the IROFS to reliably perform its function, and the effects of its failure. The description of each IROFS within an ISA Summary should identify the management measures, such as maintenance, training, and configuration management that 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 in the ISA Summary. 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 required reliability. The management measures should ensure 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 ensured 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 facility. In particular, for IROFS whose availability is to be relied upon, the time interval between surveillance observations or tests of the item should be stated, since restoration of a safe state cannot occur until the failure is discovered.

Table A-13 in Appendix A to this chapter is one example of a tabular description of IROFS meeting these criteria.

#### (7) Quantitative Standards for Chemical Consequences

The applicant's description in the ISA Summary of proposed quantitative standards used to assess consequences from acute chemical exposure to licensed material or chemicals incident to the processing of licensed material is acceptable, provided the following criteria are met:

- a. Unambiguous quantitative standards exist for each of the applicable hazardous chemicals that meet the criteria of 10 CFR 70.65(b)(7) on site, corresponding to, and consistent with, the quantitative standards in 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 10 CFR 70.61(b)(4)(i) addresses 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 could result in death for some workers, consistent with the methods used for the U.S. Environmental Protection Agency's - "Acute Exposure Guidelines--40 CFR Part 68."

- c. The quantitative standards for 10 CFR 70.61(b)(4)(ii) and 10 CFR 70.61(c)(4)(i) will correctly categorize all exposures that could lead to irreversible or other serious, long-lasting health effects to individuals. As with criterion (b), above, the standard selected should have appropriate conservatism.
- d. The quantitative standard for 10 CFR 70.61(c)(4)(ii) will correctly categorize all exposures that could cause mild transient health effects to an individual.

The NRC finds the use of the Emergency Response Planning Guidelines (ERPG) established by the American Industrial Hygiene Association, the Acute Exposure Guideline Levels (AEGL) established by the National Advisory Committee for Acute Guideline Levels for Hazardous Substances and exposure limits established by the Occupational Safety and Health Administration or contained in International Organization for Standardization (ISO) standards to be acceptable. If the applicant does not use a published exposure standard, or if a chemical has an unknown exposure standard, the ISA Summary must describe how an alternative exposure standard was established for use in the ISA. The ISA Summary must list the actual exposure values for each chemical, specify the source of the data (e.g., ERPG, AEGL, ISO, etc.), and provide information or a reference justifying that they meet the acceptance criteria stated above. See also Section 6.4.3.1 of this SRP.

#### (8) List of Sole IROFS

The descriptive list in the ISA Summary that identifies all IROFS that are the sole item credited as such for demonstrating compliance with 10 CFR 70.61 is acceptable if it includes:

- a. descriptive title of the IROFS;
- b. an unambiguous and clear reference to the process to which the item applies;
- c. clear and traceable references to the description of the item as it appears in the full list of all IROFS and the list of accident sequences.

(9) Definitions of “Unlikely”, “Highly Unlikely” and “Credible”

The regulation in 10 CFR 70.65 requires that the applicant’s ISA Summary must define 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. The reviewer should focus on objective qualities and information provided concerning accident likelihoods.

The regulation in 10 CFR 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 are 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”

The regulation in 10 CFR 70.65 requires that the applicant define the term “credible.” This term is used in 10 CFR 70.61, which requires that all credible accident sequences for which the consequences could exceed the performance requirements of 10 CFR 70.61 must be controlled to be unlikely or highly unlikely, as appropriate. If an event is not credible, IROFS 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 IROFS. There is a danger of circular reasoning here. In the safety program embodied in Subpart H to 10 CFR Part 70, the fact that an event is not “credible” must not depend on any facility feature that could credibly fail to function, or be rendered ineffective as a result of a change to the system. Each facility feature that is needed to ensure that accident events are sufficiently unlikely is an 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 some other controls or features of the plant that are not IROFS. Such an evaluation would be inconsistent with 10 CFR 70.61(d). However, it may be that an accident sequence, although not meeting a definition of “not credible”, may meet the standards for “highly unlikely” or “unlikely” due to an infrequent external initiating event, without the use of IROFS. In such a case IROFS are not necessary, but information is needed showing that the event does qualify as “highly unlikely” or “unlikely”.

Any one of the following three independent acceptable sets of qualities could define an event as not credible:

- a. An external event has a frequency of occurrence that can conservatively be estimated as less than once in a million years

- b. A process deviation consists of a sequence of many unlikely events or errors for which there is no reason or motive. In determining that there is no reason for such errors, a wide range of possible motives, short of intent to cause harm, must be considered. Complete ignorance of safe procedures is possible for untrained personnel, which should be considered a credible possibility. Necessarily, no sequence of events should be categorized as not credible if it has actually occurred in any fuel cycle facility.
- c. There is a convincing argument, given physical laws, that the process deviations are not possible, or are unquestionably extremely unlikely. The validity of the argument must not depend on any feature of the design or materials controlled by the facility's system of IROFS or management measures.

Such a demonstration of "not credible" 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 they meet the following criteria:

- a. are reasonably clear and based on objective criteria;
- b. can reasonably be expected to consistently distinguish accidents that are highly unlikely from those that are merely unlikely; and
- c. categorizes events as "highly unlikely" or "unlikely" yielding results reasonably consistent with quantitative information and quantitative criteria such as those given in the example here.

The phrase "objective criteria" means the extent to which the method relies on specific identifiable characteristics of a process design, rather than subjective judgments of adequacy. Objective criteria are needed to achieve consistency. Consistency means the degree to which different analysts obtain the same results when they apply the method. This is important to maintain an adequate standard of safety because ISAs of future facility modifications may be performed by individuals not involved in conducting the initial ISA. An acceptable qualitative method of likelihood evaluation should yield results comparable to the examples of evaluation methods given in the appendices to this chapter.

#### 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 are not necessarily complete, but contain many of the factors that are most commonly encountered. Some of these qualities relate to the characteristics of individual IROFS, such as the following examples:

- a. safety margin in the controlled parameter, compared with process variation and uncertainty
- b. whether the IROFS is an active engineered control, a passive engineered control, an administrative control, or an enhanced administrative control
- c. the type and safety grading, if any, of management measures applied to the control

- d. fail-safe, self-announcing, or surveillance measures to limit down time
- e. failure modes
- f. demand rate
- g. failure rate

Other reliability qualities relate to characteristics of the IROFS or system of IROFS, protecting against the following accident sequences as a whole among others:

- h. defense-in-depth
- i. degree of redundancy
- j. degree of independence
- k. diversity
- l. vulnerability to common-cause failure

Methods of likelihood evaluation and definitions of the likelihood terms “unlikely” and “highly unlikely” may mix qualitative and quantitative information. Certain types of objective quantitative information may be available concerning specific processes in a facility. Examples of such objective quantitative information include the following:

- a. reports of failure modes of equipment or violations of procedures recorded in maintenance records or corrective action programs
- b. the time intervals at which surveillance is conducted to detect failed conditions
- c. the time intervals at which functional tests or configuration audits are held
- d. for a fail-safe, monitored, or self-announcing IROFS, the time it takes to render the system safe
- e. demand rates (i.e., the frequency of 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 multiple IROFS.

#### Acceptance Criteria for Likelihood Indexing Methods

One acceptable 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 to this chapter shows the use of such a method, which primarily relies on a qualitative evaluation of reliability and 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. Then, the definitions of “highly unlikely” and “unlikely” would then be

acceptable limiting values of this likelihood index. For example, “highly unlikely” could be defined as: “having a risk index value less than or equal to minus 5.” And “unlikely” could be defined as: “having a risk index value less than or equal to minus 4.”

#### 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, 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 explicitly addresses several reliability and availability qualities:

- 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,” in the phrase “at least two unlikely, independent and concurrent changes,” sometimes more than 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, to qualify as “unlikely to fail.” A single simple administrative control, regularly challenged, and without any special safety margin or enhancement, where a single simple error would lead to an accident, would not qualify as “unlikely to fail.” Likewise, two simple administrative controls without special margins or enhancements, particularly of their independence, would not normally qualify as “highly 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.” One example of acceptable quantitative guidelines is given below. These guidelines serve two purposes. Specifically, these guidelines can be used as acceptance criteria for quantitative definitions of “highly unlikely” and “unlikely”, if provided by an applicant.

#### Quantitative Guidelines

A discussion of quantitative guidelines here does not imply that quantitative demonstration of compliance with 10 CFR 70.61 is required. The NRC has provided various guidance, including a Strategic Plan that bears on assuring that exposures of individuals to NRC regulated hazards, such as radiation, are acceptably infrequent. For example, the NRC Strategic Plan has a

performance goal of “no inadvertent nuclear criticalities”. The quantitative guidelines for definitions of “highly unlikely” and “unlikely”, as used in 10 CFR 70.61, given below were developed so as to be reasonably consistent with other relevant NRC guidance.

#### Highly Unlikely

Among other considerations, the guideline for acceptance of the definition of “highly unlikely” has been derived as the highest acceptable frequency that is consistent with the performance goal of having no inadvertent nuclear criticality accidents. This guideline is thus applied in considering the 10 CFR 70.61 requirement that high consequence events be highly unlikely, because such events may involve high radiation doses, as is often true for criticality accidents. To within an order of magnitude, this is taken to mean a definition that translates to a frequency limit of less than one such accident in the industry every 100 years. This results in a guideline limiting the frequency of any individual accident to  $10^{-54}$  per-event per-year. As the goal is to have no such accidents, the expectation is that most accidents would be expected to have frequencies substantially below this guideline when feasible.

#### Unlikely

Intermediate consequence events include significant radiation exposures to workers (those exceeding 0.25 Sieverts or 25 rem). The NRC has a strategic goal that there be no increase in the rate of such significant exposures. This guideline has been interpreted here to correspond to a range between  $10^{-4}$  and  $10^{-5}$  per-event per-year.

#### Quantitative Guidelines for Use with Acceptance Criteria

The applicant’s quantitative definitions of the terms “unlikely” and “highly unlikely,” as applied to individual accident sequences identified in the ISA, are acceptable to show compliance with 10 CFR 70.61 if they are reasonably consistent with the following quantitative guidelines:

Likelihood term of 10 CFR 70.61	Guideline
Unlikely	Less than $10^{-4}$ per-event per-year
Highly Unlikely	Less than $10^{-54}$ per-event per-year

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. Note that the word “unlikely” as it appears in 10 CFR 70.61(c) does not have the same meaning as when that word is used in the definition of double contingency. See Chapter 5 of this SRP.

### 3.5 Review Procedures

Organization of the reviews addressed by this chapter of the 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 the applicant’s safety program and ISA commitments, there may only be a primary ISA reviewer. However, for an initial ISA Summary submittal, the 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 review of safety program commitments, including commitments pertaining to the ISA and ISA Summary (a renewal or amendment application), 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, the application will not be accepted for review.

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 sufficient information is not present, the ISA Summary will not be accepted for review.

### **3.5.2 Safety Evaluation**

#### *3.5.2.1 Evaluation of Safety Program and ISA Commitments*

The reviewer examines the descriptions and commitments to program elements in the application or other documents for the Areas of Review 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 ISA reviewer must coordinate his or her review, with reviews being conducted under other chapters of this SRP.

#### *3.5.2.2 Evaluation of ISA Summary*

Evaluation of the ISA Summary to determine if the acceptance criteria of Section 3.4.3.2 have been met would normally be performed by a team consisting of a primary reviewer together with specialists in each category of accidents. These categories of accidents depend on the facility but, in general, are nuclear criticality, 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 his or her 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 10 CFR 70.61 should be undertaken by separate specialists for each category of accidents (i.e., nuclear criticalities, fires, radiological releases, and chemical accidents). As indicated in Appendix A to this chapter, one acceptable format for the ISA Summary is to separately tabulate or give logic diagrams for accident sequences in each accident category.

After a preliminary team review of the ISA Summary, a visit to the facility **should be made by the team** to become familiar with the three-dimensional geometry of process equipment, to review components of the ISA, and to address any issues that arose during review of the ISA Summary.

To select a subset of the accident sequences reported in the ISA Summary for more detailed review, the reviewer should look at the applicant's tabulation of high and intermediate consequence accident sequences and the types of IROFS designated for each. High consequence accident sequences protected by administrative controls should be examined very carefully, whereas intermediate consequence accident sequences protected by redundant passive engineered controls warrant a lesser degree of scrutiny. The reviewers should use the following approach to select specific accident sequences and IROFS for more detailed evaluation.

The reviewer should evaluate potential accidents using information supplied in the ISA Summary. The applicant's method for identifying and establishing the consequences and likelihood of an accident sequence may provide information sufficient for this purpose. The NRC reviewer may evaluate the accidents using qualitative screening criteria analogous to Table A-6 in Appendix A of this chapter. Other more rigorous reliability or consequence analyses may be performed as deemed necessary. On the basis of this analysis, accidents will be categorized. The reviewer may select to examine in greater detail the engineered and administrative controls for accidents in the category of highest consequences. While onsite, the reviewer should also select for specific evaluation a small sample of accident sequences determined by the applicant either to result in less than intermediate consequences or to be not credible.

From the list of the IROFS, the reviewer should categorize IROFS so that items of a similar nature are grouped together. The reviewer should then ensure that he or she has fully understood ~~one~~ one or more prototype IROFS selected from each category. For these selected prototypes, the reviewer may, if necessary, request additional information to completely understand a particular IROFS. For complex processes, the reviewer may need to visit the facility to reach an adequate understanding of how the IROFS work for the process.

### 3.5.2.3 Onsite ISA Review

The reviewer should plan on visiting the applicant's facility at least once as part of the application review process. This visit should be scheduled after the applicant's ISA Summary has received a preliminary review. The visits will enable the reviewer to confirm through detailed examination of the ISA and ISA documentation that the ISA method were selected and applied in a reasonable and thorough manner to all facility processes, that all credible high and intermediate consequence accident sequences were correctly identified, that accident sequence consequences and likelihoods were reasonably determined, and that appropriate IROFS and supporting management measures have been proposed. By means of a "horizontal" review and several "vertical" slice reviews (defined below) of processes selected by the reviewer, the completeness and adequacy of the applicant's ISA method can be established. The reviewer may use the ISA documentation to perform independent evaluations of process hazards and accident sequences using methods selected from NUREG-1513, Appendix A to this SRP chapter, or other NRC guidance.

The reviewer should not attempt a comprehensive, all-encompassing review of every facility process and every accident sequence on the site visit. Rather, the reviewer should use the site visit to confirm the appropriateness and adequacy of the applicant's ISA method and the completeness of the ISA and accuracy of analysis of accident sequences by means of a "horizontal" review and several "vertical" slice reviews of selected processes. The site visit will

also afford the reviewer an opportunity to seek answers to questions from the applicant (or possibly the ISA team) that may have arisen in the preliminary review of the ISA Summary.

The following sections discuss each of the three facets of the onsite ISA review ~~are discussed below~~.

#### (1) ISA Methods Review

The purpose of the ISA methods review is two-fold: (1) to ensure that the applicant selected appropriate ISA methods for each facility process, and (2) to ensure that the methods were correctly applied in conducting the ISA. The ISA Summary should describe the ISA methods and give a few examples of the application of the ISA methods. The ISA methods review should answer any questions that a reviewer may have concerning ISA methods and procedures after completing a preliminary review of the ISA Summary. In reviewing process-specific information in the ISA Summary and ISA documentation maintained onsite, a few processes and accident sequences should be selected to review the adequacy of the selected ISA methods and its/their application. The reviewer should examine any procedures, checklists, or guidance documents that the applicant may have onsite as guidance to ISA team members to ensure a complete understanding of the applicant's ISA methods. The reviewer should then examine the ISA documentation, including the selected processes and accident sequences, showing how the ISA methods were applied as part of the horizontal and vertical slice reviews discussed below.

#### (2) Horizontal Review

The basic purpose of the horizontal review is to ensure completeness of the ISA of facility processes. This does not require an absolute check-off of ISA documentation against the full list of processes to be covered, but does mean that a substantial fraction of the processes should receive a brief examination.

The reviewer should consult the ISA and ISA documentation to answer questions or to resolve outstanding issues resulting from the preliminary review of the ISA Summary. ~~If the ISA Summary includes sufficiently detailed information for a process, further examination of the onsite ISA documentation may not be required.~~ In particular, the reviewer should examine safety information that is not included in the ISA Summary. For example, ISA documentation related to hardware IROFS, such as system schematics and/or descriptive lists, should contain sufficient detail about hardware IROFS, such that it is clear to the reviewer what components (such as cables, detectors, alarms, valves, piping, etc.) are included within the boundary of the hardware IROFS system and would therefore be subject to management measures specified by the applicant. In addition, such documentation should also identify support systems (such as backup batteries, air supply, steam supply, etc.) on which the IROFS depends to perform its intended function. The reviewer should also examine a few processes to confirm that all accident sequences were considered and that those having potential consequences exceeding the performance requirements of 10 CFR 70.61 are included in the ISA Summary.

#### (3) Vertical Slice Review

The purpose of the vertical slice review is to examine how the ISA methods were applied to a selected subset of facility processes. For this subset of facility processes, the reviewer should examine the underpinnings of calculations, conclusions, and the design of safety programs that result from the ISA as well as safety information that is not identified in the ISA Summary. The reviewer should examine accident sequences for this subset of processes to determine the adequacy of the applicant's consequence and likelihood determinations. In addition, the reviewer

should examine the appropriateness and robustness of designated IROFS and the suitability of proposed management measures.

The ISA Summary will have categorized accidents according to their consequences, likelihoods, and IROFS. The reviewer should select a subset of processes for vertical slice review these categories. The subset should include accident sequences with relatively high levels of consequence and likelihood and accident sequences to which IROFS of different types and relatively low robustness are designated. For ISAs where the index method of Appendix A is used, and where the index scoring for all accident sequences is readily available to the reviewer, in principle, these index scores could be used to establish sequences of relatively higher risk. However, if the ISA only declares as IROFS a set of controls that are minimally necessary to demonstrate compliance with 10 CFR 70.61 likelihood requirements, then such index scores would be misleading. Instead, for selection of processes or sequences for the vertical slice reviews, one may need to use other objective qualities of the processes. For example, the selection might be based on experience or potential consequences as in the following: 1) criticality accidents in solution systems, solvent extraction process upsets, or using plutonium or high enriched uranium; 2) chemical processes involving large quantities of toxic chemicals that are highly reactive, flammable, or volatile, or are exceptionally toxic. Vertical slice reviews should be performed on processes for which less robust IROFS are designated (e.g., those with greater reliance on administrative rather than engineered controls). Again, if only a minimal set of IROFS is declared, it may be backed-up by more robust controls that are not IROFS; hence are not documented in the ISA Summary. Still, a quick review of sets of IROFS that are purely administrative, or are otherwise known from experience to be unreliable, may be advisable.

While onsite, the reviewer may confirm the adequacy of sample accident analyses that the applicant included in the ISA Summary. However, the reviewer should focus on processes and/or accident sequences that were not included as sample accident analyses in the ISA Summary to ensure the completeness of the ISA.

The vertical slice review should address any specific questions the reviewer may have related to the ISA methods. If the applicant's methods are evaluated as effective in these selected cases, there is greater assurance that they will be effective for other processes. If questions or weaknesses are discovered that may be of a generic nature, the reviewer may have to perform vertical slice analyses on several additional processes. However, a specific question on the ISA of one process may not imply that there is a generic question requiring further examination. The purpose of the vertical slice reviews is not complete verification of ISA implementation.

The total number of vertical slice reviews to be conducted will depend on the facility's total number of accident sequences for which the consequences could exceed the performance requirements of 10 CFR 70.61, the diversity of the types of processes and types of IROFS at the facility, and the results of initial reviews of the ISA Summary and the horizontal and vertical slice reviews. For most fuel fabrication facilities, the reviewer should plan on conducting vertical slice reviews for 5 to 10 NCS-significant processes, 1 to 3 fire-significant processes, and 1 to 3 chemical/radiological/environmental-significant processes. But if the initial reviews of the ISA Summary and the horizontal and vertical slice reviews identify significant issues, then additional vertical slice reviews may be warranted. **Ultimately, in order to approve the ISA and ISA program the reviewer must attain reasonable assurance that they have been implemented in compliance with the regulations.**

Each vertical slice review should include (1) familiarization of the reviewer with the safety design of the selected process and (2) examination of all onsite documentation related to the ISA of that process. If the content of the documentation leaves certain issues unclear, interviews with facility personnel may be necessary. The review should focus on the information onsite that is not

provided in the ISA Summary, but is key to determining compliance with 10 CFR 70.61 requirements.

Following the horizontal and vertical slice reviews, if outstanding questions remain about compliance with the performance requirements of 10 CFR 70.61, the reviewer may conduct an independent evaluation using appropriate methods selected from NUREG-1513, Appendix A to this chapter, or other agency guidance. The purpose of such an independent review is to identify strengths and weaknesses of the applicant's ISA methods or implementation practices, not simply to check compliance in this one case per se.

The reviewer should take care to document findings and evaluations made during this process.

### 3.6 Evaluation Findings

In general, the review findings should state that the requirements of 10 CFR 70.64, if a new facility, 10 CFR 70.65 for content, and 10 CFR 70.66 for approval have, or have not, been met, and why they have, or have not, been met. There should be a finding statement, following the evaluation of each specific area of review, stating how and why the information submitted in that area complies with the related regulatory requirement, if so. Specifically, the reviewer's(s') findings in the SER should state conclusions of the types described in the following paragraphs:

- general conclusion resulting from the reviewer's evaluation of safety program commitments:

The NRC staff concludes that the applicant's safety program, if established and maintained pursuant to 10 CFR 70.62, is adequate to provide reasonable assurance that IROFS will be available and reliable to perform their intended safety function when needed and in the context of the performance requirements of 10 CFR 70.61.

General findings for each of the areas of review should state how the applicant's information demonstrates compliance with the acceptance criteria of Section 3.4.3.1. If the reviewer finds that the acceptance criteria are not met, ~~the reviewer should recommend a license condition rectifying the deficiency, and the applicant is not in compliance with the regulations, then the situation must be rectified before approval can be given.~~ If the applicant has submitted an adequate explanation of an alternative way of complying with the regulations, the NRC's SER should contain a finding that the alternative is acceptable to meet the basic regulatory requirement addressed.

- general conclusions resulting from the staff's evaluation of an ISA Summary: Many hazards and potential accidents can result in unintended exposure of persons to radiation, radioactive materials, or toxic chemicals incident to the processing of licensed materials. The NRC staff finds that the applicant has performed an ISA to identify and evaluate those hazards and potential accidents as required by the regulations. The NRC staff has reviewed the ISA Summary and other information, and finds that it provides reasonable assurance that the applicant has identified IROFS and established engineered and administrative controls to ensure compliance with the performance requirements of 10 CFR 70.61. Specifically, the NRC staff finds that the ISA results, as documented in the ISA Summary, provide reasonable assurance that the IROFS, the management measures, and the applicant's programmatic commitments will, if properly implemented, make all

Formatted: Indent: Left: 0.92", Tab stops: 0.92", Left + Not at 0"

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 Part 70 that address the nine 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).

Findings may be made concerning compliance of specific processes with requirements of 10 CFR 70.61 or other parts of the regulation, for those processes that receive specific detailed review. However, such findings should be limited to a finding of reasonable assurance that a process having the IROFS, 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. 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.

U.S. Environmental Protection Agency, "Acute Exposure Guidelines," 40 CFR Part 68, Appendix A.

U.S. Nuclear Regulatory Commission, "Nuclear Fuel Cycle Facility Accident Analysis Handbook, NUREG/CR-6410, March 1998.

U.S. Nuclear Regulatory Commission, "Integrated Safety Analysis Guidance Document," NUREG-1513, May 2001.