From: "FARRELL, Clifton" <CWF@nei.org>
To: "'btm1@nrc.gov'" <btm1@nrc.gov>
Date: Fri, Aug 6, 1999 3:35 PM
Subject: NEI Comments on Draft SRP Chapter 3

Barry:

Attached are three files (each in HTML and MS-Word format) that contain NEI's comments on Chapter 3 of the June, 1999 edition of the draft SRP (NUREG-1520). The underlined text and struck-through text has been manually inserted and so I hope that it will all be legible in the HTML conversion. The difference between the "NRC" and "Final" files is that the former contains all of the struck-through text and proposed addition text and the latter had been cleaned of all the struck-through text. In other words, the latter "Final" file reflects what NEI would like the final version of Chapter 3 to look like. Would you please "doctor up" the covering letter in the same way as you did to that sent with the Chapter 1 & 2 comments. It looks excellent.

Please be in touch if you experience any problems in retrieving any of the documents.

Best Regards,
Clifton

<<SRP (June 1999 Version) Cover Letter4>> <<Cover Letter (Ch. 3)>>

<<SRP (June 1999 Version) Sec. 3 (NRC)>> <<SRP Chapter 3 -- NRC>>

<<SRP (June 1999 Version) Sec. 3 (Final)>> <<SRP Chapter 3 -- Final>>

Felix M. Killar, Jr.
DIRECTOR, MATERIAL
LICENSEES & NUCLEAR INSURANCE
Tel: (202) 739-8126

August 6, 1999

Mr. Theodore S. Sherr
Chief, Regulatory and International Safeguards Branch
U.S. Nuclear Regulatory Commission
Two White Flint North 8A33
Washington, D.C. 20555

Reference: Comments on the June, 1999 Draft Version of NUREG-1520 '*Standard Review Plan for the Review of a License Application for a Fuel Cycle Facility*': Chapter 3 – Integrated Safety Analysis (ISA)

Dear Mr. Sherr:

The Nuclear Energy Institute (NEI)[1] and its industry members are undertaking detailed reviews of each chapter of the draft Standard Review Plan (SRP) released on June 2, 1999 as part of SECY-99-147. To provide effective guidance on implementation of 10 CFR 70, we believe the SRP should be concisely written and accurately reflect the 'risk-informed, performance-based' regulatory approach incorporated into the Part 70 rule revisions.

Accompanying this letter are NEI's comments on Chapter 3 ('*Integrated Safety Analysis (ISA)*') of the draft SRP. The review is presented in two parts: (i) general comments on the sub-chapter, and (ii) specific language (or stylistic) improvements presented on a red-lined version of the draft SRP sub-chapter. In view of the number and complexity of NEI's proposed improvements, a second copy of SRP Chapter 3 has been prepared from which the red-lined text deletions have been

[1] NEI is the organization responsible for establishing unified nuclear industry policy on matters affecting the nuclear energy industry, including the regulatory aspects of generic operational and technical issues. NEI's members include all utilities licensed to operate commercial nuclear power plants in the United States, nuclear plant designers, major architect/engineering firms, fuel fabrication facilities, materials licensees, and other organizations and individuals involved in the nuclear energy industry.

removed. This version of draft SRP Chapter 3 will enable you to more clearly understand the improvements which NEI is recommending.

NEI is pleased that many improvements to the draft SRP developed in public meetings and workshops and proposed by industry have been incorporated into this latest draft of the SRP. The June, 1999 revision is markedly improved over earlier versions issued in 1998 and we compliment the staff for this accomplishment.

We look forward to working with you and your staff to make NUREG-1520 a clear and concise document that will facilitate implementation of the new provisions of 10 CFR Part 70. Please feel free to contact me should you have any questions concerning the proposed improvements in the attachment to this letter.

Sincerely,

Felix M. Killar, Jr.
Director, Material Licensees and Nuclear Insurance

c. Mr. Marvin S. Fertel
Dr. Carl J. Paperiello, Director NMSS

Ref: I:\Files\Part 70\SRP (June 1999 Version) Cover Letter4.msw

COMMENTS ON THE JUNE, 1999 DRAFT VERSION OF NUREG-1520 '*STANDARD REVIEW PLAN FOR THE REVIEW OF A LICENSE APPLICATION FOR A FUEL CYCLE FACILITY*'

CHAPTER 3: INTEGRATED SAFETY ANALYSIS (ISA)

I. General Comments

NEI recommends a substantial revision of draft SRP Chapter 3 to incorporate the changes made to 10 CFR Part 70. Proposed revisions to 10 CFR Part 70.62 have significantly changed how a license applicant's Safety Program is to be evaluated. The adequacy and acceptability of an applicant's Safety Program will now encompass review of three items:

- commitments pertaining to the ISA
- ISA Summary
- management measures

Exclusion of the results of the ISA from a facility's licensing basis makes redundant to the license reviewer a majority of the content of the June, 1999 revision of draft SRP Chapter 3. Rather than conduct a detailed review of the complete ISA, the license reviewer will now review the docketed ISA Summary. The ISA Summary must present sufficient information to enable the reviewer to understand how the ISA was performed, the qualifications of the team performing the ISA, the major, safety-significant results of the ISA and the procedures to maintain the ISA. Much of the guidance in the June, 1999 revision of the SRP on how to conduct an ISA, and especially the detailed guidance on establishing qualitative standards for the likelihood and consequence of an accident sequence, should be excluded. However, this guidance is valuable and should be considered for incorporation into NUREG-1513 ('*ISA Integrated Safety Analysis Guidance Document*').

NEI recommends that Chapter 3 be restructured into two principal sections: **ISA Commitments** and **ISA Summary**. Chapter 3 would, therefore, provide guidance in evaluation of these first two components of the safety program review. SRP Chapter 11 will provide the reviewer with guidance on evaluation of the third component of the safety program – management measures for items relied on for safety. The ISA Summary section of Chapter 3 should provide guidance in preparation of this document in accordance with the requirements of 10 CFR Part 70.65(b). The purpose and use, scope, format and content of the ISA Summary would all be presented in detail.

Draft SRP Chapter 3 Appendix A details an approach for *quantitative* risk evaluation in an ISA. NEI recommends that a second appendix, Appendix B, be developed that outlines a comparable *qualitative* approach for risk evaluation. Appendices A and B would together provide the license applicant and NRC reviewer

with two acceptable methods for risk evaluation. As risk evaluation of credible accident sequences is performed as part of the ISA (rather than the ISA Summary), NEI recommends that Appendices A and B be removed from draft SRP Chapter 3 and incorporated instead into NUREG-1513 ('*ISA Integrated Safety Analysis Guidance Document*'). NUREG-1513 should become the principal guidance document for conducting an ISA. NEI has not yet drafted an Appendix B for qualitative risk evaluation. Upon completion, it will be submitted to the NRC for review and possible incorporation into NUREG-1513.

The SRP contains numerous errors in terminology. Several terms such as '*consequence of concern*', '*management controls (or assurances)*', '*human-system interface analysis*', and '*safety controls*' persist even though they are no longer used or cited in 10 CFR 70. Several undefined terms are also used and should be deleted (e.g. '*incredible event*', '*mitigative barrier*'). There persists some confusing and contradictory use of the terms '*items relied on for safety*' and '*management measures*'. For consistency, the term '*safety control*' (and all variations thereof) should all be replaced by '*items relied on for safety*' to ensure no misunderstanding. The SRP is internally inconsistent in referring to materials to be submitted to the NRC for review. The terms '*ISA results*', '*ISA documentation*', '*information submitted*' and '*ISA Summary*' are frequently used interchangeably and in a manner that could confuse the reviewer. Clear distinctions must be made amongst the definitions for '*ISA documentation*', '*ISA results*' and '*ISA Summary*' and each term must be strictly defined and used accordingly. The NRC has attempted to incorporate the NRC-OSHA Memorandum of Understanding into this chapter, but there are several instances where the third principle ('*chemical risks from plant conditions which affect the safety of licensed material*') is mis-stated or lacking. Use of reactor terminology persists (e.g. '*unreviewed safety question*' in §3.4.3(9)) whereas the correct reference should be to the §70.72 facility change mechanism. Finally, the SRP still makes extensive use of '*consequence*' and '*likelihood*' and little reference to '*risk*' – a deficiency that should be remedied. These inconsistencies and terminology errors can all be addressed by means of a thorough and critical technical editing of the chapter.

To reflect the significant change in the content of SRP Chapter 3, NEI recommends that it be entitled '**Integrated Safety Analysis (ISA) Commitments and ISA Summary**'.

NEI recommends that Chapter 3 be significantly condensed through removal of a majority of the detailed guidance on conducting an ISA. Chapter 3 should be structured to allow license applicants to commit to performance indicators rather than to specific detailed procedures explaining how a particular performance goal will be achieved. As such, the prescriptive detail in the June, 1999 revision of Chapter 3 should also be deleted.

Finally, NEI strongly encourages the NRC to draft SRP Chapter 3 in a much more concise and straightforward manner. Deletion of repetitive language, tightening of the language, consistency with 10 CFR 70 terminology and definitions and removal of the prescriptiveness will facilitate use by the applicant and reviewer without detracting from the importance of the guidance. The review should focus on assessment of an applicant's commitments and proposed performance indicators and not on specific details outlining how a particular performance goal will be met.

In summary, the following structural changes are proposed for SRP Chapter 3:

- delete guidance on conducting an ISA. Transfer to NUREG-1513
- delete guidance on evaluation and assessment of an ISA
- delete Appendix A ('*Quantitative Risk Assessment*') and transfer to NUREG-1513. Prepare a new Appendix B ('*Qualitative Risk Assessment*') to complement Appendix A and append to NUREG-1513
- structure Chapter 3 into two sections (i) ISA license commitments, and (ii) ISA Summary. Include guidance on evaluation and assessment of each
- add guidance on structure of an ISA Summary (contents, format) as directed in 10 CFR Part 70.65(b)
- re-name chapter '*Integrated Safety Analysis (ISA) Commitments and ISA Summary*'

II. Specific Comments

Specific comments are noted on the attached copy of draft SRP Chapter 3.

Ref: I\Files\Part 70\SRP (June 1999 Version) Sec 3.msw (NRC)

3.0 INTEGRATED SAFETY ANALYSIS (ISA) COMMITMENTS AND ISA SUMMARY

3.1 PURPOSE OF REVIEW

The purpose of this ~~the ISA~~ review is to establish reasonable assurance that the applicant or licensee will establish and maintain a safety program for the licensed facility that will satisfy the performance requirements of 10 CFR Part 70.61. A facility's safety program has three components: (i) maintenance of process safety information, (ii) performance and maintenance of an integrated safety analysis (ISA), and (iii) implementation of management measures that will ensure the availability and reliability, when required, of items relied on for safety identified in the ISA. The review conducted in Chapter 3 will address the first two components of the facility's safety program (process safety information, ISA). The third element of the safety program (management measures) will be assessed separately in Chapter 11 of this SRP.

The review is structured into two sections:

Section 1: Commitments	assessment of an applicant's commitments to undertake and maintain various analyses and databases, to implement corrective actions when safety-significant deficiencies are identified and to make informational reports to the NRC within specific timeframes
Section 2: ISA Summary	review of the ISA Summary to ensure identification of safety-significant external hazards and credible accident sequences whose consequences could exceed the performance criteria of 10 CFR 70.61, establishment of comparative risks, designation of appropriate items relied on for safety and implementation of acceptable management measures

Materials to be examined in the review include a list of license commitments pertaining to the ISA and the ISA Summary. The reviewer should understand that the applicant will have previously conducted an ISA, the results of which, including all supporting documentation (e.g. piping and instrumentation drawings (PI&Ds), dose calculations, drawings, ISA worksheets, criticality safety evaluations, etc.), will be maintained at the facility site. The ISA is not part of the license application and requires neither assessment nor approval by the reviewer. The applicant will also have prepared a summary of the ISA ('*ISA Summary*') that presents analyses of safety- and risk-significant issues identified at the facility. The ISA Summary is not part of the license application, but is submitted to the NRC for placement on the docket. Review of the ISA Summary is required to provide reasonable assurance to the reviewer that the applicant has identified significant hazards at the facility, analyzed potential, credible accident sequences and implemented appropriate safety controls to prevent or mitigate such accidents. If deemed necessary, the reviewer may consult the ISA or background and supporting information not contained in the ISA Summary. For example, the reviewer may wish to review specific process criticality safety evaluations, the detailed results of an accident sequence analysis, the technical justification for selection of a particular risk classification method or the characteristics of a low-risk accident sequence not discussed in the ISA Summary.

~~1. Performed a comprehensive ISA of the fuel cycle facility and its processes using effective systematic methods.~~

~~2. Identified and evaluated all hazards and credible accident sequences in the ISA involving process deviations or other events internal to the plant (e.g., explosions and fires), and credible external events (e.g., floods, high winds, and earthquakes) that could result in consequences to the public, worker, or the environment of the types specified in 10 CFR 70.61.~~

~~3. Designated engineered and administrative items relied on for safety, and evaluated the set of items for each accident sequence to provide reasonable assurance, through preventive or mitigative measures, that the safety performance requirements of 10 CFR 70.61 are met.~~

~~4. Used competent staff in the ISA process.~~

~~5. Provided a formal system to manage changes to the ISA.~~

3.2 RESPONSIBILITY FOR REVIEW

Primary: FCLB assigned reviewer

Secondary: Technical specialists in specific areas

Supporting: Fuel Facility Inspection Staff

3.3 AREAS OF REVIEW

The staff initially reviews the applicant's proposed license commitments pertaining to the ISA. This is followed by a detailed review of the ISA Summary.

3.3.1 License Commitments

Staff review of the applicant's safety program commences with examination of proposed license commitments. These commitments specifically pertain to the ISA and are in addition to other commitments the applicant will have made on other health and safety issues. This review must provide reasonable assurance that the applicant has committed to:

1. Compile and maintain current a database of process safety information that includes information pertaining to the hazards of materials used or produced in the process, information pertaining to the technology of the process and information pertaining to the equipment used in the process

2. Develop and implement procedures to keep the ISA and ISA Summary accurate and up-to-date. The applicant commits to maintaining the ISA as the facility's safety basis. The applicant commits to promptly analyzing and incorporating into the ISA any changes in the process safety information, operating procedures, process design bases, control systems or variables, instrumentation, items relied on for safety, management measures, etc., to revising the ISA, as required, and to submitting changes in the ISA Summary to the NRC in accordance with the schedule in 10 CFR 70.72(d)(1).

3. Address promptly any safety-significant process vulnerabilities or unacceptable performance deficiencies identified in the ISA

4. Design and implement a corrective action program to address any deviations from safe operating conditions (as defined in the SRP Glossary), accidents or other abnormal operational events that are encountered

5. Design and implement a facility change mechanism process whereby any proposed change to the process, operating procedures, flowsheet, items relied on for safety or their management measures is first evaluated by the ISA methodology to establish its risk and safety-significance and to determine the need for a license amendment.

6. Engage suitably qualified and trained personnel to apply the ISA methodology, both in conducting the initial ISA and in performing updates when required

7. Maintain items relied on for safety for higher-risk accident sequences to ensure their reliability and availability when required

8. Implement an emergency preparedness program for use in the event an item relied on for safety or a management measure fails

9. Maintain a log at the facility that documents any item relied on for safety or management measure that failed to perform its function when required or when tested

3.3.2 ISA Summary

3.3.2.1 Purpose and Scope

The ISA Summary presents a succinct synopsis of the results of the ISA. The ISA Summary focuses on safety-significant features of a facility which could potentially pose the greatest risks to human health and safety and the environment. It presents a sub-set of the facility hazards and accident sequences analyzed in the ISA and tabulates both the items relied on for safety proposed by the applicant to prevent or mitigate such accidents and the management measures to ensure their reliability and availability when required.

The ISA Summary differs from the ISA in two substantive ways. The ISA Summary:

- discusses hazards and accident sequences at a *systems level* (*versus* at a component level in the ISA)
- focuses on high- and intermediate-consequence events that could exceed the performance requirements of 10 CFR Part 70.61 (*versus* consideration of *all* low- to high-risk accident sequences in the ISA)

The ISA Summary is intended to be a “stand-alone” document that succinctly distills from the ISA:

- ISA methodology
- ISA study team (members & qualifications)
- descriptions of facility processes, identification of process hazards and assessments of general types accident sequences
- risk classification approach for ranking general types of accident sequences

- high- and intermediate-risk accident sequences
- items relied on for safety for high- and intermediate-consequence events
- management measures applied to items relied on for safety

The level of technical and engineering detail in the ISA Summary is considerably less than in the ISA. For example, the ISA Summary requires descriptions of only the *general types* of credible accident sequences and not the detailed descriptions of each accident sequence assessed in the ISA. The ISA Summary relies more on *narrative text* and schematic flow diagrams rather than on detailed technical information and data analysis. It should be structured to "walk" the primary reviewer through the plant's operations and individual processes. In doing so, the reviewer should be able to understand the principle of operation of the facility, recognize facility and process hazards, identify items relied on for safety to prevent or mitigate an accident and understand selection of management measures applied to such items relied on for safety. The reviewer should, as a result, be able to judge the adequacy of the applicant's safety program.

3.3.2.3 Format and Content

The ISA Summary should be structured into three sections and present the following information:

(i) General Information	information of a general nature applicable to all processes analyzed in the ISA, such as: • facility and site descriptions • ISA methodology(ies) • selection of appropriate exposure standards • ISA study team • definition of terms
(ii) Process-Specific Information	summary of risk and safety assessments of each facility process including: • processes analyzed • process hazards • general types of accident sequences • risk assessment of general types of accident sequences • items relied on for safety • management measures
(iii) Items Relied on For Safety	tabulations of items relied on for safety for safety-significant, general types of accident sequences

Information in the ISA Summary should primarily be excerpted from the ISA. Information that should be expected in each section of the ISA Summary is summarized below:

3.3.2.4 ISA Summary Review Topics

~~Information about the licensee's ISA is contained in the license application, the ISA summary, and other ISA documentation. The application and the ISA summary are submitted to NRC whereas additional documentation of the ISA is available for NRC review at the facility site. The term "results of the ISA" includes all the ISA information that is submitted to NRC plus the additional supporting information that is found on-site. In general, the application contains information needed by the reviewer to understand the nature of the ISA process performed at the site, the qualifications of the team performing the ISA, the major results of the ISA, and the procedures for conducting and maintaining the ISA. The application provides licensee commitments that demonstrate the adequacy of the ISA program. The summary of the ISA provides a synopsis of the results of the ISA as specified in 70.65(b). Information contained in the ISA summary that also satisfies the information requirements in the application may be referenced in the application.~~

~~The staff reviews the application and the ISA results (ISA summary and other ISA documentation) to find reasonable assurance that the applicant has performed a systematic evaluation of the hazards and credible accident sequences. The review includes the makeup of the ISA team and the administrative and physical safety controls required to prevent or mitigate the consequences of accidents. The review boundary includes those accidents that result in a release of licensed radioactive material or an inadvertent nuclear criticality event. In addition, the staff reviews accidents involving hazardous chemicals when the chemicals are composed of, or produced from the processing of, licensed radioactive material; or if the accident has the potential to jeopardize the safety of regulated activities. An event sequence having consequences less than those identified in 10 CFR 70.61(c) would not require further consideration within the ISA.~~ The areas of review for the ISA Summary are as follows:

(i) General Information

1. The site description (see Section 1.3, "Site Description") concerning those factors that could affect safety, such as geography, meteorology (e.g., high winds and flood potential), seismology, and demography.

2. The facility description (see Section 1.1, 'Facility and Process Description') concerning features that could affect potential accidents and their consequences. Examples of these features are facility location, facility design information, and the location and arrangement of buildings on the facility site.

3. The ISA study team that conducted the ISA, including the technical areas of expertise represented on the team and a description of the team's experience and qualifications in conducting ISAs.

~~3. The description of each process analyzed as part of the ISA. Specific areas reviewed include basic process function and theory, major components their function and operation, process design and equipment, and process operating ranges and limits.~~ [Comment: this review item is relocated to the second category of information ('*Process-specific Information*') in the ISA Summary.]

~~4. The applicant's commitment to compile and maintain a current and accurate set of process safety information (PSI) 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").~~ [Comment: this review item is relocated to the second category of information ('*Process-specific Information*') in the ISA Summary.]

~~5. The description of the applicant's requirements for ISA team training and qualifications (Section 11.3, "Training and Qualification").~~ [Comment: this review item is relocated to the second category of information ('*Process-specific Information*') in the ISA Summary.]

4~~6~~. The ISA method(s) used in conducting the ISA to identify hazards, forecast accident sequences and to predict their consequences and likelihoods of occurrence ~~for each individual process node and the justification for its selection. For purposes of this review, the ISA begins with an identification of hazards (chemicals, radiological materials, fissile materials, etc.) that may present a potential threat to the public, facility workers, or the environment. Based on a systematic analysis of each plant process, the ISA Process Hazard Analysis (PHA) identifies a set of individual accident sequences or process upsets that could result from the hazards. The review of the ISA methodology includes evaluating the applicant's methods in the following specific areas:~~

~~a. Hazard identification.~~

~~b. Process hazard analysis (accident identification).~~

~~c. Accident sequence construction and evaluation.~~

~~d. Consequence determination and comparability to 10 CFR 70.61.~~

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

5. The definitions of terms used in performing the ISA, including those for the terms 'credible', 'unlikely', 'highly unlikely' and 'likely'

6. The quantitative standards used in the ISA to establish permissible acute exposures to licensed material or hazardous chemicals produced from licensed materials

(ii) Process-Specific Information

1. The tabulation of all processes analyzed in the ISA.

2. The safety assessment of each process. The process safety assessment will include the following components:

   a. process description (narrative description and a simple block flow diagram)

   b. hazard identification

   c. general types of accident sequences (identified in the ISA process hazard analysis)

   d. unmitigated consequences of each general type of accident sequence, their comparison to the performance requirements of 10 CFR Part 70.61(b) and (c) and their ranking in terms of risk.

   e. likelihood of occurrence of each general type of accident sequence

f. risk classification of each general type of accident sequence

3. The description of items relied on for safety to prevent or mitigate each general type of accident sequence's risk to an acceptable level (so that the performance criteria of 10 CFR 70.61 are not exceeded), including classification by type (engineered or administrative controls) and, if applicable and explanation of how such items were graded according to their safety-importance.

4. The management measures applied to each item relied on for safety and, if applicable, a description of how such measures were graded

5. The compliance with the nuclear criticality monitoring requirements of 10 CFR 70.24

6. The description of how the design of new facilities or new processes at existing facilities adheres to the baseline design criteria of 10 CFR 70.64.

7. ~~The narrative description, process hazard analysis documentation, and the tabular summary of the ISA results in the following specific areas:~~

   a. ~~The list of hazardous materials and conditions resulting from the Hazard Identification task.~~

   b. ~~The Hazard Interaction Matrix table [see reference AIChE 1992, section 3.3].~~[Comment: too prescriptive. Delete.]

   c. ~~Accident sequences identified by the ISA systematic Process Hazard Analysis.~~ [Comment: too prescriptive. Delete.]

   d. ~~Unmitigated and mitigated consequences of each postulated accident to facility workers or the public.~~

   e. ~~Comparisons of the consequences of each postulated accident to the consequences of concern identified in 10 CFR Part 70.61.~~ [Comment: the term 'consequence of concern' is no longer used in 10 CFR 70.] Delete.]

   f. ~~Identification of engineered and administrative controls involved in each accident sequence.~~

   g. ~~Assignment of accident sequences to likelihood categories and comparison to 10 CFR 70.61 requirements.~~

8. ~~The description of the engineered and administrative safety controls, and mitigative barriers used to maintain safe operation of the facility to ensure that, for each accident sequence, the controls are commensurate with 10 CFR 70 requirements as interpreted in the acceptance criteria of section 3.4 below. These criteria are risk informed in that systems of controls applied to accident sequences having more severe consequences are to be correspondingly more reliable. The applicant should also commit to maintain safety controls and mitigative barriers available and reliable for high and intermediate risk accident sequences.~~

9. The management measures (see definition in Glossary) applied to each safety control needed to conform to the requirements of 10 CFR 70.62(d). Those management measures that are generically applied to all safety controls or to specified classes of controls may be described in Section 11, "Management Controls Systems," or in Sections 4 through 7 and 9, which cover specific safety disciplines. However, since the ISA identifies the safety controls as such, and provides other information needed to apply management measures in a graded manner, the information from the ISA summary and other ISA documentation needed to implement these systems should be reviewed.

   For accident sequences evaluated as potentially having the consequences specified in 70.61, but meeting the likelihood requirements of 10 CFR 70.61 without controls, staff reviews the basis for the applicant evaluation of the sequence as being of acceptably low likelihood. Typically such accident sequences involve very low likelihood natural phenomena or other initiating events.

10. The facility procedures for conducting and maintaining the ISA. The object of this review is to ensure the overall integrity of the ISA as a current and accurate safety basis for the facility. Specific review areas include the applicant's procedures for: (1) performing and updating the ISA, (2) review responsibility, (3) documentation (including provisions for updating NRC on changes to controls or seeking NRC approval of changes per 70.72, and (4) maintenance of ISA records per 70.62(a)(2). The integrity of the ISA procedures should be controlled by the applicant's configuration management program. [Comment: 10 CFR 70.65 no longer requires a detailed description as to how the ISA will be maintained. This is a licensee commitment and need not be discussed here. Delete this paragraph.]

(iii) Items Relied on For Safety

1. The tabulation of all items relied on for safety that are required for each general type of accident sequence analyzed in the ISA, as well as any other safety controls or safeguards that the applicant has designated to be items relied on for safety

2. The tabulation of any item relied on for safety that is the sole item preventing or mitigating a general type of accident sequence that exceeds the performance requirements of 10 CFR Part 70.61

3.4 ACCEPTANCE CRITERIA

3.4.1 Regulatory Requirements

The requirement to describe the applicant's safety program, including both the ISA Summary and appropriate management measures, is specified in 10 CFR 70.65(a). The three components of the safety program are defined in 10 CFR 70.62(a). Licensee commitments to perform an Integrated Safety Analysis (ISA) using current process safety information and to keep the ISA updated and current as the facility's safety basis are ~~is~~ specified in 10 CFR 70.62. ~~10 CFR 70.62(c) specifies requirements for the tasks comprising the ISA and the demonstration that items relied on for safety meet the safety performance requirements of 70.61.~~ 10 CFR 70.72 states requirements for keeping the ISA and its documentation current when changes are made to systems, structures, and components.

3.4.2 Regulatory Guidance

Guidance applicable to performing an ISA and documenting the results is contained in NUREG-1513, "Integrated Safety Analysis Guidance Document." A sample ISA Summary for one process is also available to illustrate an acceptable form and content. [Comment: this example of an ISA Summary is incomplete and does not address all of the requirements of 10 CFR 70.65(b). Must be corrected.]

3.4.3 Regulatory Acceptance Criteria

3.4.3.1 License Commitments

~~The acceptance criteria for an ISA are based on meeting the relevant requirements in 10 CFR Part 70, "Domestic Licensing of Special Nuclear Material." The ISA will form the basis for the safety program by identifying accidents of concern, designating controls and management measures, and evaluating the likelihood of each accident sequence for compliance with 70.61. The staff will accept the ISA, the designation of controls, and the management of the ISA process if the reviewer finds~~ The staff will find an applicant's safety program commitments acceptable if the following criteria are met:

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

    a. the hazards of all materials used or produced in the process. Information on chemical and physical properties such as toxicity, acute exposure limits, reactivity, chemical and thermal stability such as is included on Material safety Data Sheets (meeting the requirements of 10 CFR 1910.1200(g)) should be provided.

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

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

2. The applicant commits to keeping the ISA and ISA Summary accurate and up-to-date by means of a suitable configuration management system. The ISA must account for any changes made to the facility or its processes (e.g. changes to the site, operating procedures, control systems). Management policies, organizational responsibilities, revision timeframe and procedures to perform and approve revisions to the ISA should be outlined succinctly. The applicant commits to evaluating any facility changes or changes in the process safety information that may alter the parameters of an accident sequence by means of the facility's ISA methodology. The applicant commits to using an ISA Team with similar qualifications to that used in conducting the original ISA for any modifications and revisions that the applicant deems necessary. The applicant commits to review of any

facility changes that may increase the level of risk and, if dictated by revision of the ISA, to select and implement new or additional items relied on for safety and appropriate management measures. The applicant commits to submitting to the NRC revisions of the ISA Summary within the timeframe specified in 10 CFR 70.72(d)(1).

3. The applicant commits to promptly address any safety-significant vulnerabilities or unacceptable performance deficiencies identified in the ISA. Whenever an update of the ISA is conducted, the applicant commits to taking prompt and appropriate actions to address any vulnerabilities that may have been identified. If a proposed change results in a new type of accident sequence (e.g. different initiating event, significant changes in the consequences) or increases the risk of a previously analyzed accident sequence to an unacceptable level, the applicant commits to promptly evaluating the adequacy of existing items relied on for safety and associated management measures and to making necessary changes, if required.

4. The applicant commits to design and implement a corrective action program that will promptly address, implement and document appropriate responses to accidents, deviations from safe operating conditions and recommendations for process improvements. The program should be structured to address potential process vulnerabilities as well as actual accidents and incidents which have occurred. It should also be structured to respond to deficiencies identified in compliance audits. Facility policies to encourage the identification and reporting of process vulnerabilities (e.g. equipment malfunctions, problems with safety systems) or areas in which assurance of worker health and safety could be reasonably enhanced should be described. Procedures to describe internal evaluation of incidents should be described. The applicant should discuss the key components of the corrective action plan (e.g. investigative team, documentation of findings, implementation of corrective actions)

5. The applicant commits to design and implement a facility change mechanism that meets the requirements of 10 CFR 70.72. The applicant should discuss the key components of the written facility change mechanism such as: evaluation of the change within the ISA framework, prediction of impacts on worker health and safety, modifications to operating procedures, change authorization procedures, updating the facility ISA.

6. The applicant commits to engage personnel with appropriate experience and expertise in engineering and process operations to update and maintain current the ISA. The ISA team shall consist of individuals knowledgeable in the facility's ISA methodology and in process hazards analysis.

7. The applicant commits to installation of items relied on for safety (including administrative controls) and maintaining them in a functional state so that they are available and reliable when needed. Management measures (which are evaluated in SRP Chapter 11) comprise the principal mechanism by which the reliability and availability of items relied on for safety is assured.

8. The applicant commits to design and implement an emergency preparedness program for use in the event an item relied on for safety or management measure fails. The applicant's emergency preparedness program should outline emergency actions that employees are to perform in the event of a serious event (e.g. fire, unintentional release of licensed material or hazardous chemicals produced from licensed material, inadvertent nuclear criticality). The applicant's written emergency preparedness program should outline procedures to address, for example, pre-planning for emergency conditions, preparation of emergency

plans, specification of employee actions in an emergency, worker evacuation, solicitation of off-site emergency response assistance.

9. The applicant commits to maintaining a log at the facility, in accordance with the requirement of 10 CFR 70.62(a)(3), that documents each discovery of an item relied on for safety or management measure that has failed to perform its function. The applicant commits to enter into the log following information such as: item relied on for safety or management measure that failed, affected safety functions, affected facility process(es), cause(s) of the failure, corrective or compensatory action(s) taken.

3.4.3.2 ISA Summary

The staff will find an applicant's safety program description as presented in the ISA Summary to be acceptable if the following criteria are met:

(i) General Information

1. The description of the site ~~for processing nuclear material~~ is considered acceptable if the applicant includes or references the following ~~safety-related~~ information ~~in the application~~:

   a. A description of the site geography, including its location in relation to ~~from~~ prominent natural and man-made features such as mountains, rivers, airports, population centers and possibly hazardous commercial and manufacturing facilities~~, etc. adequate to permit evaluation of the likelihood and magnitude of consequences of concern~~.

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

   c. Characterization of natural phenomena (e.g., tornadoes, hurricanes, and earthquakes) and other external events sufficient to assess their impact on plant safety and to assess their likelihood of occurrence. ~~The discussion identifies the design basis events for the facility and indicates which events are considered incredible and the basis for that determination. The assessment also indicates which events could occur without adversely impacting safety.~~

   d. An appropriately-scaled plan map of the facility showing the 'controlled area' as defined in 10 CFR 20.1003 with supporting narrative text that explains how this area will be maintained and how activities of the public will be excluded or controlled.

The ISA Summary may reference information on the site contained in the ISA or submitted as part of the required data for SRP Chapter 1.3 ('*Site Description*'). ~~The level of detail for this material is greater than that which would be acceptable in the general information in Chapter 1.~~

2. The description of the facility is considered acceptable if the applicant includes or references the following information:~~identifies and describes the general features that are relied on or required for safety. If such information is available elsewhere in the application, reference to the appropriate sections is considered acceptable. The information provided should adequately support an overall understanding of the facility structure and its general~~

~~arrangement as it pertains to the ISA. As a minimum, the applicant adequately identifies and describes:~~

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

b. Design information regarding the resistance of the facility to failures caused by credible external events, when those failures may produce consequences of concern.

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

The ISA Summary may reference information on the facility contained in the ISA or submitted as part of the required data for SRP Chapter 1.1 ('*Facility Description*'). The facility description is used to systematically evaluate the spatial relation between a process accident and the people and the environment that could be adversely affected. While there may be some duplication in the information included in the site description, the facility description should generally focus more on how plant structures and configurations may cause or impact the progression of an accident and how they may impact worker and public safety.

The siting and design of a facility may significantly impact the progression and outcome of an accident sequence in areas such as the following:

- number of workers potentially impacted
- off-site environmental impacts (e.g. proximity to rivers (unconfined spills or sizable leaks), nearby population centers, fires (ignitable reagents))
- airborne contamination (e.g. site topography and nearby terrain, predominant wind directions)
- extreme weather events (e.g. direct flooding, lightening and high winds, loss of power, loss of containment of waste holding ponds)
- on-site chemical storage (e.g. toxic release hazards (NH_3, Cl_2, UF_6, etc.), separation of caustics from acids and corrosives, storage tank separation distances (storage dikes, sumps, drains, waste, etc.))
- vehicle traffic flow patterns
- access and egress, evacuation routes, emergency exits (e.g. access for maintenance, sampling, repairs, access to hydrants, monitor and control valves)
- protection of piping and vessels from external impacts
- process piping corrosion protection (compatibility with corrosive acids)
- spill control (e.g. drainage directions and destinations, sumps, perimeter dikes, automated leak detection systems, treatment capacities)
- fire protection (e.g. ignition sources (transient and fixed), control of combustible materials and reagents, fire barriers, explosion hazards, appropriate fire fighting equipment (CO_2, halon), shielding of water-based fire suppression systems adjacent to or in moderation controlled areas)
- personal protective equipment (e.g. locations of SCBA/airline respirators, safety showers and eyewash locations)
- spatial interactions

[Comment: The following paragraph of text has been deleted. Its substance has been relocated to section (ii) of this SRP §3.4.3.2.]

3. The description of the processes analyzed as part of the ISA is considered acceptable if it describes the following features sufficiently to permit: 1) an evaluation of the completeness of the hazard (accident) identification task, and 2) an evaluation of the likelihood and consequences of the accidents identified. If the information is available elsewhere in the application and is adequate to support the ISA, reference to the appropriate sections is considered acceptable. The information provides an adequate explanation of how the safety controls reliably prevent the process from exceeding safety limits for each case identified in the ISA results where they are needed.

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

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

   c. Process design and equipment. This information includes a discussion of process design, equipment, and instrumentation that is sufficiently detailed to permit an adequate understanding of the results of the ISA. It includes schematics indicating safety interrelationships of parts of the process. In particular, either schematics or descriptions indicating the location and geometry of Special Nuclear Materials, moderators, and other materials in the process are sufficient to permit an understanding of the adequacy of controls on mass, geometry, moderation, reflection, and other criticality parameters affected by geometry.

   d. Process operating ranges and limits. This information includes the operating ranges and limits for measured process variables (e.g., temperatures, pressures, flows, and compositions) used in engineered or administrative controls to ensure safe operation of the process. The process operating limits and ranges are considered acceptable if they are consistent with those evaluated as adequate for safety in the ISA. One acceptable way of presenting this information is as a tabular summary of all safety controls grouped according to hazard type, i.e. nuclear criticality, radiological hazards, chemical hazards, etc., as shown in Appendix A, Table A.3-7.

[Comment: The following paragraph is deleted. The substance of this paragraph is a "commitment" which has been addressed in §3.4.3.1 of the SRP.]

4. For purposes of conducting an ISA, the applicant's Process Safety Information is considered acceptable if the applicant commits to maintain, at a minimum, the following information current and accurate:

   a. Hazardous material information including toxicity information, permissible exposure limits, physical data, reactivity data, corrosivity data, and stability data (thermal and chemical).

   b. Process technology information including block flow diagrams or simplified process flow diagrams, process chemistry, maximum intended inventory, and safe upper and lower limits for parameters controlled for safety reasons, such as temperatures, pressures, flows, and compositions.

~~c. Process equipment information including materials of construction, piping and instrumentation diagrams (P&IDs), electrical classification, relief system design and design basis, ventilation system design, design codes and standards used, material and energy balances, and safety systems (e.g., interlocks, detection systems, and suppression systems).~~

3. The description of the ISA team that prepared the ISA is considered acceptable ~~5. The ISA team for each process analyzed is considered acceptable~~ if the following criteria are met:

   a. The ISA team ~~has a team~~ leader ~~who~~ is formally trained and knowledgeable in the ISA methodology and ~~chosen for the hazard and accident evaluations. In addition, the team leader~~ can demonstrate an adequate understanding of all process operations and hazards under evaluation.~~, but is not the cognizant engineer or expert for that process.~~ [Comment: unnecessarily prescriptive. Delete.]

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

   c. ~~The t~~Team members represent a variety of process operating and engineering design experience, in particular, radiation safety, nuclear safety, fire protection, and chemical safety disciplines.

   d. A manager provides overall administrative and technical direction for the ISA.[Comment: the ISA Team, leader could fulfill the role of '*manager*'. A separate individual may not be required.]

The ISA Summary may reference information on the ISA Team that is contained in the ISA. The ISA Summary should highlight the technical areas of expertise represented on the team and include a description of the team's experience and qualifications in conducting ISAs.

4~~6~~. The descriptive summary of the ISA methodology is considered acceptable if it describes the methods used for each ISA task, and the basis for selection of each method, so that the adequacy of the method is clear and appropriate according to the criteria described in NUREG-1513 for selection of ISA methods. The method used to perform the ISA must have adequately addressed the four ISA components: (i) hazard identification, (ii) process hazard analysis, including accident sequence construction and evaluation against the performance criteria of 10 CFR 70.61, (iii) specification of items relied on for safety, and (iv) recommendation of management measures. Staff will find the ISA methodology acceptable if the following criteria are met: ~~Specific acceptance criteria for the ISA methodology are as follows:~~

a. The selected hazard identification method is ~~selected~~ considered acceptable if it:

i. Incorporated the process safety information for the facility, and specifically, information pertaining to the hazards of licensed material and other hazardous chemicals used or produced by the process, the technology of the process (e.g. process chemistry, safe limits for operating parameters, consequences of process deviations) and equipment used in the process (e.g. PI&Ds, ventilation system design, safety systems, etc.). ISA methods may include, for example, "*Hazard and Operability Analysis (HAZOP)", "What If Analysis," "Fault Tree Analysis," "Preliminary Hazards Analysis*" or a combination of one or more of such approaches. Any commercial software packages used in the analysis should be identified. Finally, if the ISA was performed in accordance with specific industry standard or with one endorsed by a professional organization (e.g. American Institute of Chemical Engineers), these standards should be identified. ~~Provides 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). The list includes maximum intended inventory amounts and the location of the hazardous materials at the facility.~~[1].[2][Comment: the requirement to list hazardous materials has been addressed in section (ii). Footnotes are overly prescriptive and should be deleted.]

ii. Determine~~s~~d potential interactions between materials or between materials and conditions that could result in hazardous situations.

i. Considered credible external factors (e.g. meteorological, seismological, hydrological) as initiators of accident sequences that could pose a threat to facility workers, the public or the environment

b. The selected process hazard analysis ~~(accident sequence identification)~~ method ~~selected~~ is considered acceptable if:

i. Its selection was ~~is~~ consistent with the guidance provided in NUREG-1513. ~~For methods used by the applicant but not addressed in NUREG-1513, the applicant provides justification and references for their use.~~

ii. It adequately address~~ed~~ all the hazards identified in the hazard identification task of section 4~~6~~.a above. The applicant identifies and justifies any hazards eliminated from further consideration.

i. The applicant has provided acceptable qualitative or quantitative definitions of terms used in evaluating the likelihood of occurrence of an accident sequence (e.g. 'likely', 'unlikely', 'highly unlikely') and in defining what constitutes a 'credible accident sequence'). The definition for 'credible' will likely incorporate some reference to the likelihood of the accident occurring. In general, a 'credible' accident is one that has

---

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

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

some non-negligible probability of occurrence during the reference timeframe. An accident sequence may be characterized as 'credible' if there is an upset condition associated with the process that can reasonably be expected to occur. For example, exceeding concentration or mass limits or violating favorable geometry parameters (bottle volumes) or violating spacing limits are all credible upset conditions that could lead to an inadvertent nuclear criticality incident. Such an accident sequence would be deemed 'credible.' An 'incredible' event, in contrast, has a likelihood of occurrence approximating zero during the reference timeframe.

iv~~iii~~. It provides reasonable assurance that the applicant identifies ~~all~~ significant types of accident sequences (including the items relied on for safety ~~controls~~ used to prevent or mitigate the accidents) that could exceed the performance criteria ~~result in consequences of concern~~ identified in §70.61. [Comments: (1) the adjective 'all' has been deleted as no method can provide complete assurance that all types of accident sequences have been identified. (2) Issues of chemical process safety are thoroughly addressed in SRP Chapter 6.]

v~~iv~~. It takes into account the interactions of identified hazards and proposed items relied on for safety ~~controls~~, including system interactions, to ensure that the overall level of risk at the facility is consistent with the requirements of §70.61 and appropriately limited.

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

~~vi. It addresses hazards resulting from process deviations (e.g., high temperature, high pressure), initiating events internal to the facility (e.g., fires or explosions), and hazardous credible external events (e.g., floods, high winds, and earthquakes, airplane crashes). The applicant provides justification for its determination that certain events are incredible and, therefore, not subject to analysis in the ISA.~~ [Comment: this section is redundant. Paragraph (ii) already states that all hazards identified by the paragraph (i) task will be addressed. Furthermore, if a hazard is deemed inconsequential, paragraph (ii) will have allowed the applicant to already have deleted it from further consideration. The term '*incredible*' is undefined. Delete this paragraph (vi) as redundant.]

~~vii. It adequately considers initiation of, or contribution, to accident sequences by human error by appropriate use of human-systems interface analysis.~~ [Comment: "human-systems interface analysis" was deleted from consideration as an SRP Chapter 11 management measure. Operator error will have already been considered in the process safety information data. Delete paragraph (vii) as redundant.].

~~viii. It adequately considers common mode failures and system interactions in evaluating systems that are to be protected by double contingency.~~ [Comment: common mode failures and system interactions will have been considered in paragraph (iv) above. Double contingency protection will also have been addressed in paragraph (iii) above as simply a special case of ensuring suitable items relied on for safety are in place to protect against the event whereby two unlikely, independent and concurrent changes occur in process conditions.]

s have been used in

assessing general types of accident sequences. Appropriate qualitative or quantitative

methods have been used to forecast both the likelihood and consequences of each type of accident sequence. The applicant also states which quantitative acute exposure standards were used for hazardous chemicals. Nuclear criticality consequences may have been estimated through use of standard American Nuclear Society or equivalent standard methods. Environmental, industrial and chemical consequences, including fire and explosion, may have been estimated with the assistance of material safety data sheets, chemical interaction information and computer modeling techniques including emission calculations and air dispersion models. Each type of unmitigated accident sequence is compared to the performance criteria of 10 CFR 70.61 and should any fall into the high- or intermediate-consequence event categories, the applicant has recommended appropriate items relied on for safety. ~~as described in the appropriate safety chapters of the license application (e.g., Section 5.0, "Nuclear Criticality Safety," Section 6.0, "Chemical Safety"). Acceptable methods of consequence evaluation are described in Nuclear Fuel Cycle Facility Accident Analysis Handbook, NUREG/CR-6410, March 1998.~~[Comment: the foregoing citation, while important, is relevant to the conduct of an ISA and should, therefore, be transferred to NUREG-1513] A ranking of the general types of accident sequence *by risk* should be included in the application.

d. The applicant demonstrates that an effective method was used to provide reasonable assurance that the recommended administrative or engineered safety controls (items relied on for safety) will ensure that the risk of any accident sequence will not exceed the performance criteria of 10 CFR 70.61~~uses, and submits adequate documentation of, for evaluating the adequacy of items relied on for safety in all identified accident sequences~~. [Comment: there is no regulatory requirement to specify items relied on for safety for accident sequences that can reliably be demonstrated to not exceed the performance requirements of 10 CFR 70.61]. ~~This evaluation method is considered acceptable if:~~.

~~i. For nuclear criticality accident sequences, it can demonstrate adherence to the double contingency principle, including reasonable assurance that common failure modes are accounted for (see Section 3.4.3.8), or~~

~~ii. It can demonstrate compliance with the graded protection criteria of 10 CFR 70.62(a) consistent with the guidance in the Appendix A. Or, for individual accident sequences not conforming to the guidance in Appendix A, specific and adequate justification showing conformance to 10 CFR 70.61 is provided.~~

[Comment: there remains no need to single out an inadvertent nuclear criticality for special treatment. Section (i) should be deleted. Section (ii) is applicable to the ISA and not to the ISA Summary. Delete this section as well.]

e. The applicant used acceptable quantitative standards to establish permissible acute exposures to licensed materials or hazardous chemicals produced from licensed materials. The chosen acute exposure standards should be identified and a brief, supporting explanation provided supporting the selection. Numerical acute exposure limits for those principal chemical compounds analyzed in the ISA accident sequences (e.g. HNO_3, UF_6, HF, etc.) should be tabulated. Any chemical compounds for which an Alternate Concentration Limit (ACL) was used in the ISA should be identified and a brief explanation substantiating its use provided.

(ii) Process-Specific Information

1. The facility process tabulation is acceptable if all processes analyzed in the ISA are properly identified and referenced to the facility description.

2. The safety assessment of each process is acceptable if the following information is provided:

   - a narrative description of the process that is sufficiently detailed to enable the reviewer to understand the process' theory of operation. This description should provide an overview of the basic process function, major process components (e.g. mixing, sintering, neutralization), process inputs and outputs (e.g. reagents, licensed material forms, products, wastes) and an explanation of how the process integrates with other facility process operations. This information, which should be summarized from the ISA, may be supported with process schematics, simple block flow diagrams, chemical flow sheets or tables of information. A brief statement of the safety basis(es) of the process as applicable to each of the generic hazards should be included. For example, in discussing a general type of accident sequence that could result in an inadvertent nuclear criticality, parameters that are controlled (e.g. geometry, concentration, mass, etc.) should be specified and credible accident sequences associated with the process (e.g. exceeding concentration or mass limits, violating favorable geometric parameters or bottle spacings, etc.) should be stated. The description should limit the amount of quantitative information.
   - identification of all hazards for the process resulting from process deviations (e.g. volume, concentration, temperature), initiating events internal to the facility (e.g. fire) and credible external events (e.g. floods, hurricanes). Hazards of particular interest are those listed in 10 CFR 70.65(b)(3): radiological, chemical and facility hazards
   - a list of general types of accident sequences identified in the process hazard analysis. Brief narrative text should explain each generic accident type, including the initiating event(s). Note that specific accident sequences should not be listed. General types of accident sequences for different initiating hazards may include, for example:

Initiating Hazard Type	General Type of Accident Sequence
Radiological	"loss of moderation control due to water ingress" "radiological exposure of workers to airborne uranium"
Chemical	"breakage of a control valve on a UF6 cylinder resulting in an inadvertent release of uranium hexafluoride"
Facility	"worker injury caused by moving parts in pug mills" "ignition of hydraulic lubricating oils"

   - specification of the unmitigated consequences of each general type of accident sequence, linkage to the initiating event(s)
   - likelihood of occurrence of each general type of accident sequence. The likelihood may be expressed in either a qualitative or quantitative manner based on the method used in conducting the ISA
   - risk classification of each general type of accident sequence. Risk is computed to be the product of the consequence and the likelihood forecast for the general type of accident. The comparative risk of the general type of accident sequence is established through comparison against the performance criteria of 10 CFR 70.61

3. The description of the items relied on for safety is acceptable if the applicant:

- identifies which general types of accident sequence require items relied on for safety to reduce their risk to acceptable levels. High consequence events forecast to be highly unlikely or intermediate consequence events forecast to be unlikely do not require application of any items relied on for safety. Similarly, no items relied on for safety are required for general types of accident sequences that are neither high- or intermediate-consequence events.
- enumerates *at the systems level* appropriate items relied on for safety that, when applied to a general type of accident sequence, will provide reasonable assurance that the performance requirements of 10 CFR 70.61 will be met. Selection of appropriate items relied on for safety will depend upon the safety bases and parameters that are used to control a process.
- classifies each items relied on for safety as one of the following:

    (1) **administrative control**: operation requires human intervention for operation (e.g. oversight of sampling program, maintenance of logs of SNM, sealing of drums, timing of addition of reagents, visual inspection of leaks)
    (2) **augmented administrative control**: administrative control that relies on a warning device to notify an operator that intervention is necessary to implement a control (e.g. solution level alarm)
    (3) **active engineered control**: controls that use active sensors and that require no operator intervention to operate (e.g. in-line concentration monitors, automatic valve closures, tank level controls or automatic shut-off valves, solution pH controller)
    (4) **passive engineered control**: controls that use only fixed design features and that require no operator intervention to operate (e.g. compatibility of materials of construction with solutions, dikes and secondary containment pits, deadman valves, multiple evacuation routes, storage of flammable liquids in NFPA-approved storage cabinets)

- explains how the item relied on for safety will prevent or mitigate an accident sequence
- explains how any items relied on for safety were graded according to their safety importance in accordance with 10 CFR 70.62(a)

4. The description of management measures is acceptable if the applicant:

- proposes suitable management measures for item(s) relied on for safety for each general type of accident sequence so as to provide continuing assurance of compliance with the requirements of 10 CFR 70.61
- briefly describes the management measures applied to each generic type of accident sequence and classifies each as active engineered, passive engineered, administrative or augmented administrative
- explains how the management measure will provide reasonable assurance that the items relied on for safety will be reliable and available to perform its safety function, when required
- explains how management measures were graded according to the reduction of risk attributable to a particular safety control or control system in accordance with 10 CFR 70.62(d)

5. The description of methods to comply with the nuclear criticality monitoring requirements of 10 CFR 70.24 is acceptable if the applicant:

    - provides a narrative description of the criticality monitoring system and information that demonstrates its capability to detect the minimum radiation levels in 109 CFR 20.24(a)
    - provides a suitably-scaled plan drawing of the location of criticality detectors and alarms relative to process operations in which accident sequences potentially leading to inadvertent nuclear criticalities were identified in the ISA

6. The description of how the design of a new facility or of a new process at an existing facility (including proposed items relied on for safety) adheres to the baseline design criteria of 10 CFR 70.64 is acceptable if the applicant:

    - outlines how compliance with the ten criteria listed in 10 CFR 70.64(a) has been established:
        (a) quality assurance and records: explanation of how management measures were selected to ensue that items relied on for safety will be reliable and available when required to perform their function and commitments to retain records on the performance and maintenance of such management measures
        (b) natural phenomena hazards: protection against external, natural hazards at a level equivalent to the most severe, documented historical event at the facility (e.g. floods, hurricanes, winds)
        (c) fire protection: protection against fires and explosions
        (d) environmental and dynamic effects: protection against environmental conditions; protection from dynamic events associated with normal facility operations (e.g. operation, maintenance, testing) and postulated, credible accidents
        (e) chemical protection: protection against chemical risks produced from licensed material, plant conditions that affect the safety of licensed material and hazardous chemicals produced from licensed material
        (f) emergency capability: design features to maintain control of licensed material, to ensure the safe evacuation of on-site personnel and the availability of both on-site and off-site emergency services and facilities (e.g. hospitals, fire prevention)
        (g) utility services: provision of emergency utility services when required
        (h) management measures: inspection, testing and maintenance programs for items relied on for safety
        (i) nuclear criticality controls
        (j) instrumentation and controls: for monitoring and controlling the behavior of items relied on for safety
    - demonstrates adherence to defense-in-depth design practices including a preference for engineered controls over administrative controls and implementation of procedures that limit challenges to items relied on for safety

[Comment: The entire paragraph 7 of draft SRP Chapter 3 (pp. 3.0-9 through 3.0-17) is deleted. The information provided in this paragraph 7 guides the applicant in conducting an ISA, but not in preparing an ISA Summary. The contents of this paragraph 7 should be

considered for inclusion in NUREG-1513 (‘*ISA Integrated Safety Analysis Guidance Document*’) which should become the principal guidance document for conducting an ISA.

mary and the in-

plant documentation of results, is acceptable if it is sufficient to demonstrate that the following three top level criteria have been met:

a) completeness in identifying all accident sequences,
b) acceptable evaluation of consequences, and
c) acceptable evaluation of likelihood.

That is, the documentation of results is acceptable if it demonstrates:

(a) completeness of the ISA in identifying all hazards and accident sequences that might be capable of producing consequences of concern. This means that all accidents exceeding the minimum consequence levels of 10 CFR 70.61 including: those that involve releases of licensed material or hazardous chemicals produced from licensed material, all unplanned radiation exposures, and all nuclear criticality accidents have been identified. The primary criterion for completeness is that the systematic method chosen was correctly applied. During the PHA phase accidents will be identified whose consequences may initially be unknown, then later are analyzed and shown to be beneath the minima of concern. The ISA documentation must show which such accidents have been eliminated due to insufficient consequences, otherwise the completeness of those identified cannot be evaluated. Large groups of events of a similar nature and clearly having consequences below the level of concern may be described as a single item, provided the definition of the group is sufficiently clear as to which accidents are included, so that completeness is evident;

(b) correct evaluation of the consequences of each accident sequence and comparison to the consequence levels of concern in 10 CFR 70.61, and

(c) evaluation showing, with adequate basis, compliance with the likelihood requirements of 10 CFR 70.61.

Supporting criteria for acceptable ways of complying with each of these three top level criteria follow.

a. COMPLETENESS.

The information submitted is acceptable for showing completeness in identifying accident sequences and evaluation of consequences if:

i. The summary of the hazard identification results provides:

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

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

ii. The ISA results documentation provides either:

1) A tabular summary description of the accident sequences identified in the process hazard analysis. The tabular description consists of one row for each accident sequence. Accident sequences initiated by the same type of event, and consisting of the same sequence of control failures, and resulting in the same consequence category are summarized as a single row. This row lists the initiating event, the controls or barriers that must fail in order for the accident to occur, and the level of unmitigated consequences, if all controls fail. The listing clearly indicates the sequence and linkage between each initiating event, the controls designed to prevent or mitigate consequences of concern, and the resulting consequences when these controls fail. The tabular summary identifies the severity level of each type of consequence (radiological, criticality, chemical, environmental) according to the values defined in 10 CFR 70.61. Information sufficient for evaluation of compliance with the likelihood requirements of 10 CFR 70.61, such as likelihood indices are tabulated. Appendix A, Table A-1, provides an acceptable way of presenting this information.

OR

2) A set of logic diagrams, such as fault trees or event trees for each process, presenting the same information as in 1) above.

In the tabular summary or diagrams showing accident sequences, it is not necessary to list as a separate sequence every conceivable permutation of the accidents. The listing has three purposes: 1) to show completeness, 2) to permit evaluation of likelihood (adequacy of controls), and 3) to identify controls relied on to prevent and mitigate accidents. Accidents having characteristics that all fall in the same categories can be grouped as a single line item in the table, if: a) the initiating events have the same type of effect on the system, b) they all consist of failure of the same controls, c) they all result in violation of the safety limit on the same parameter, and d) they all result in the same type and severity category of consequences. A primary purpose of showing completeness is to assure that existing safety controls are adequate. Once this has been shown for a class of accidents having the same characteristics, it is not necessary to distinguish among the different types. On the other hand, if a different initiating event poses a different type of challenge to a safety control, then it should be listed separately, because it may reveal a weakness of the control.

To demonstrate completeness, it may be necessary to describe certain accidents evaluated as incredible events, when this is not obvious. Justification for their evaluation as incredible should be provided.

b. CONSEQUENCES.

The information submitted is acceptable for showing adequate evaluation of consequences of accidents if:

i. The ISA results documentation at the plant includes a description of each accident that includes an estimate of its quantitative consequences (doses, chemical exposures, criticality) in a form that can be directly compared to the consequence levels in 10 CFR 70.61 or includes a reference to a calculated value that applies to that accident; and

ii. The ISA Summary includes a brief description of each process that also summarizes the accident consequences in that process by giving the maximum calculated exposure values for each type of chemical and the maximum radiological dose, other than from criticalities, to both workers and the offsite public, and whether a criticality accident was identified in that process.

The ISA results documentation must show that all accident sequences have a likelihood and consequences, such that the safety performance requirements of 10 CFR 70.61 are met. Showing the consequences for each accident can be done using a tabular summary as shown in Appendix A, Table A-1, by a narrative list of all accident sequences, or by annotated logic diagrams.

Consistent with the guidance in the following paragraph, criticality accidents will normally be high consequence events because the dose will exceed 100 rem to nearby workers (see Section 5.0, "Criticality Safety"). For processes with effective engineered shielding, criticalities may produce very low doses to workers. However, as stated in the regulation, notwithstanding the effectiveness of shielding or other mitigative features, primary reliance must be on prevention of criticalities. However, when shielding is used, it is acceptable that preventive measures of lower reliability be used. That is, shielded criticality events need not be highly unlikely.

In assessing the consequences of nuclear criticality accidents to workers, since a typical criticality of 10^{17} fissions produces a dose of about 450 to 1000 rem at 2 meters, it is acceptable to assume that, absent shielding, criticalities will exceed the 100 rem threshold. Hence, all such criticalities would be categorized as "high consequence" accidents in the terminology of 10 CFR 70.61. Any reduction of the dose from a criticality accident to a value below 100 rem is acceptable if due to reliable engineered features, such as shielding. Administrative controls alone would not normally be considered of adequate reliability. In evaluating shielding, a criticality of a conservative credible magnitude must be assumed. The Nuclear Fuel Cycle Facility Accident Analysis Handbook, NUREG/CR-6410, March 1998, provides methods for estimating magnitudes of criticality events.

c. LIKELIHOOD

The ISA documentation is acceptable for showing compliance with 10 CFR 70.61 and 70.62(a) if:

1) It contains an evaluation of the likelihood of each accident that is adequately supported, and
2) these evaluated likelihoods comply with 70.61.

The likelihood requirements stated in 10 CFR 70.61 are that accidents resulting in consequences of concern in 70.61(b), "high consequences", be "highly unlikely"; and those resulting in consequences in 70.61(c), "intermediate consequences", be "unlikely".

Acceptance criterion 1 above means that, to be acceptable, the evaluation of the accidents must be supported by use of a methodology that provides reasonable assurance that the items

relied on to prevent or mitigate the accident are sufficient to achieve the regulatory requirement of unlikeliness. Such methods must be systematic, consistent among different practitioners, consistent with the actual history of failure events at the plant, and consider all the factors that affect the reliability of items. As a minimum, the method should consider the factors of redundancy, independence, concurrency, and human error. To achieve consistency, objective written methods, data, and criteria should be established to be followed by ISA Team members evaluating likelihood compliance.

Acceptance criteria 2 above means that, ultimately, the conclusion of an evaluation must clearly assign the accident as "highly unlikely" or "unlikely" as required. This means that the terms, "unlikely" and "highly unlikely", require interpretation. The applicant may provide in the ISA submittal, a definition and basis for these terms. One basis acceptable to the staff is provided in the following.

The text and tables in Appendix A describe an acceptable method for establishing likelihoods based on estimated frequencies of failure.

LIKELIHOOD CRITERIA

The terms, "highly unlikely" and "unlikely", are inherently quantitative in nature. That is, the underlying concept is that events have a certain likelihood of occurrence in any one year; and adequate safety performance means this likelihood be sufficiently low. The obvious questions are:

1) What annual frequency would qualify as "unlikely" or "highly unlikely" respectively?
2) How can compliance with the requirements be demonstrated?

10 CFR 70.61 safety performance likelihood requirements are stated in qualitative rather than quantitative form. Thus staff should not interpret these requirements as mandating that quantitative analysis be done to show compliance. However, quantitative analysis of likelihoods is one acceptable method of showing compliance. If quantitative analysis is performed, accident sequence frequencies should be determined using established methods and input values consistent with industry performance. Because quantitative methods would be acceptable, there follows a discussion of acceptable accident frequency values based on Commission guidance. Following this discussion of frequencies, criteria for acceptable non-quantitative methods will be given.

QUANTITATIVE LIKELIHOOD EVALUATION

Quantitative Evaluation Methods

Standard methods for quantitative evaluation of the frequency of accidents can be found in works on reliability engineering and probabilistic risk assessment. Such methods require input information concerning failure and repair rates for basic events. These basic events may be external or internal initiating events or failures of items relied on for safety. Quantitative credit should not be taken for the low likelihood of an event without justification. One justification is that the event is failure of an item relied on for safety that is subject to management measures (e.g. maintenance, training) to assure meeting its reliability goal. Another justification is that the event has inherently low likelihood that cannot reasonably be increased by human intervention.

Quantitative Acceptance Criteria

There are two safety performance measures established as part of the NRC Strategic Plan that bear on the question of how reliable safety controls must be. These goals thus bear directly on the question of acceptance criteria for safety controls identified in the ISA's to be done at fuel cycle facilities. The two safety performance measures are: 1) No inadvertent nuclear criticalities, and 2) no increase in reportable radiation releases. Unshielded criticality events can be expected to produce doses to workers exceeding the 100 rem value defining "high consequences". Hence, high consequence events are tied to this first safety performance measure. That is, an acceptable interpretation of the 70.61 requirement that high consequence events be "highly unlikely" should be consistent with the goal of "no inadvertent nuclear criticalities". This cannot mean zero likelihood, but neither can it mean that criticalities are expected frequently.

The second Commission safety performance measure refers to the requirements for Abnormal Occurrence reports by the NRC to Congress of radiation releases. One of these Abnormal Occurrence reporting criteria is 25 rem exposure to any adult. In terms of 70.61, 25 rem is an intermediate consequence event for a worker, and a high consequence event for the offsite public. Hence, the 70.61requirement that intermediate consequence accidents be "unlikely" is constrained by the Commission goal of "no increase" in the rate of 25 rem doses.

The current 1997 five year average of reportable radiation exposures (25 rem) is 0.4 per year. If no increase is to be permitted, then the contribution of fuel cycle facilities, which in the past has likely been zero, should be at most a small fraction of this 0.4 per year. For example, let the fuel cycle industry be allocated 10% of this value, hence 0.04 per year. If there are about 10 fuel cycle facilities, this is 0.004 per facility per year.

Similarly, to achieve no inadvertent criticalities, the expected frequency per accident per year must be sufficiently low. Let us say that, for the whole industry we wish to have a likelihood of criticality no more than once in 100 years. This would appear to be about as high a value as is tolerable for be consistent with the Commission goal. For an industry of 10 facilities, 0.01 per year is 0.001 per facility per year. Note that this is less than the 0.004 per facility per year goal for offsite doses exceeding 25 rem derived above.

Considering the above, a consistent set of quantitative goals would require that the sum of the frequencies of all accident sequences at a facility be less than:
1) 0.001 per facility per year for high consequence events, and
2) 0.004 per facility per year for intermediate consequence events.

It should be noted that the safety performance requirements of 70.61 are applied to each individual accident identified in the ISA. If an applicant chooses to use quantitative methods for evaluating compliance with 70.61, then summing the accident frequencies for the whole facility and showing compliance with the above numerical goals is one acceptable way of demonstrating compliance with the requirements.

NON-QUANTITATIVE LIKELIHOOD EVALUATION

In order that each accident sequence have sufficiently low likelihood to comply with 70.61 it is necessary that the system of safety controls (IROFS) designed to make the likelihood low have certain reliability characteristics. These characteristics include redundancy, independence, low failure rate, rapid detection of failures, and rapid restoration or repair. Qualitatively, the system of controls preventing an accident is sufficient to make it highly unlikely if it has double contingency protection as interpreted by the NRC staff. Double contingency protection can be achieved by having two independent highly reliable controls, or a larger number of redundant

controls of equivalent system reliability. Qualitatively, the system of controls preventing an accident is sufficient to make it unlikely if it has at least one highly reliable control, or multiple redundant controls of equivalent system reliability.

For an accident sequence with unmitigated consequences in the high consequence category of 70.61, adherence to double contingency is acceptable. Adherence to double contingency requires that at least two unlikely, independent, and concurrent changes in process conditions are necessary before a criticality accident can occur. If double contingency is not feasible, then the controls should exhibit sufficient redundancy and diversity to make criticality comparably unlikely.

For an accident sequence that results in the intermediate consequence category of 10 CFR 70.61, at least a single unlikely event must occur before the unmitigated consequences of the accident occur. The following is a logical deduction from the set of safety performance requirements; namely, that a mitigative control applied to a sequence must reduce the consequences below the limits defining the lower bound of the category in order to be credited in determining compliance with 70.61.

To show qualitative compliance with the likelihood requirements, the applicant must describe the qualitative likelihood evaluation method and criteria that have been used. The results of applying this method and criteria must then be documented for each accident sequence identified in the accident identification (PHA) phase of the ISA. The evaluation method must be systematic and sufficiently objective to allow different teams to produce consistent results. It is not adequate merely to have the ISA Team express a holistic judgement that the system of IROFS preventing a given accident makes it sufficiently unlikely. Such a method lacks consistency and objectivity and cannot be evaluated. The double contingency principle identifies the reliability characteristics required but does not provide criteria for when a process change is sufficiently "unlikely" to qualify.

The acceptance criterion for a non-quantitative likelihood evaluation method is that it include evaluation of each of the reliability characteristics of the system of controls. These characteristics to be evaluated are:

redundancy,
independence,
concurrency of the system,
likelihood of each of the individual "process changes".

Detailed acceptance criteria for each characteristic are given below.

Redundancy

Redundancy refers to process designs where multiple items relied on for safety must fail before an accident can occur. An effective way to make accidents highly unlikely is to provide sufficient redundancy. Double contingency is a concept that includes redundancy as one element. It may appear that double contingency only requires a twofold degree of redundancy. This is not strictly true. Some controls used to prevent accidents are not sufficiently reliable on their own to make the undesired process change qualify as "unlikely". This is particularly true when relying on administrative controls. By administrative is meant procedures requiring correct action by an operator. When using such low reliability controls, process parameters are often controlled by multiple redundant items. Though no one of them would qualify alone as "unlikely" to fail, taken together they make the process change unlikely. Thus, to achieve

double contingency may require a degree of redundancy greater than two. Two highly reliable engineered controls may be sufficient, but a greater number of controls is needed if each is of lower reliability.

Independence

Independence must be evaluated when redundancy is relied upon. Two events are independent if the likelihood of occurrence of each does not depend on the other. If independence is not achieved, then the likelihood of both failures may not be as low as one estimates. Independence means no common cause, no shared elements, and nothing else that could cause loss of both functions. There are checklists and other methodological tools for performing common cause evaluations of sets of controls. Ideally these methods should be used. In any case, independence should be evaluated. Controls that act upon the same process parameter may be subject to a single point failure that bypasses or overwhelms both. Processes which rely on correct action by an operator may be vulnerable to a single point failure that is an incorrect action by that operator. Protecting against this type of operator error may require physical locks or other means of preventing any single individual from taking an action that could be incorrect.

Concurrency

Any non-quantitative method for evaluating redundant systems of safety controls should take credit for lack of concurrency of control failures. Accidents often require that two process changes occur, each a change in the state of the system. The first change places the system in a certain state, for example, a critical mass accumulates. The second change, for example, addition of moderator, must occur while this first state still exists. If the first state is detected and corrected rapidly, it is much less likely that the second event will occur while the system is vulnerable. Thus for such active redundant systems, the evaluation methodology should include evaluation of the time to detect and correct failures. These time periods are referred to as "surveillance intervals" and "repair times". The total of these two for the first failure should be much shorter than the mean time between failures of the second control.

Another way of saying the same thing is that systems having items that may fail during the life of the plant require at least annual surveillance. Similarly, systems containing items known to fail frequently must have virtually continuous surveillance. This is not necessarily difficult because many processes are continuously manned during operation, failures are obvious, and restoration is quick. It can also be achieved by fail safe devices or by continuous automatic monitoring. The point is that the evaluation must explicitly consider surveillance and repair times. Without surveillance, failure of redundant systems containing items which can fail cannot be considered highly unlikely.

Likelihood

As stated earlier, the number of redundant items needed to make an accident highly unlikely depends on how unlikely failure of each redundant item is. All items are not created equal. In general, certain types of items are less likely to fail than others. A better way of saying this is that items with certain characteristics can more easily be made reliable. The usual hierarchy is: passive engineered controls, active engineered controls, enhanced administrative controls, and simple administrative controls. Among administrative controls another such hierarchy is: enhanced prohibitions, simple prohibitions, enhanced positive actions, and simple positive actions required for safety. Although the reliability of safety items can be roughly categorized in this way, a better way is to define groups of items graded according to their safety significance.

~~For instance the terms "safety equipment", "safety related equipment","high reliability equipment", "process features relied on for safety", etc. may be used. Equipment or features in these groups then receive sufficient management measures (e.g., maintenance, surveillance, configuration management) to assure that they achieve a reliability appropriate to their group. The point is that, to be acceptable, a method for non-quantitative evaluation of accident sequences requires that the reliability of individual safety items be assured by characteristics or measures whose presence and relative effectiveness can be objectively determined.~~

~~Appendix A describes a method for demonstrating compliance with the likelihood requirements of 10 CFR 70.61. This method, though derived from and related to underlying frequencies of failure, can be applied as a purely qualitative method.~~

(iii) Items Relied on For Safety

1. The tabulations of items relied on for safety required by 10 CFR 70.65(b) are acceptable if the applicant provides for each general type of accident sequence:

    - list of all items relied on for safety. This list should include the following information in an abbreviated form:
        - (i) information on the administrative or engineered control (e.g. nature of the expected operator response, description of the piece of safety equipment) that is applied to each general type of accident sequence
        - (ii) information on the management measures applied to the item relied on for safety and any safety grading thereof
        - (iii) if applicable, information showing compliance of the item relied on for safety with the baseline design criteria of 10 CFR 70.64(a)
    - list of items relied on for safety that are the sole item preventing or mitigating an accident sequence that could exceed the performance requirements of 10 CFR 70.61

[Comment: The entire contents of paragraph 8 of draft SRP Chapter 3 are deleted. The regulatory citation in paragraph 8 (10 CFR 70.62(c)(vi)) is incorrect as it does not pertain to the ISA Summary. The correct citation should be 10 CFR 70.65(b)(6). Only "…*a list briefly describing all items relied on for safety*…" is required.]

~~8. 70.62(c)(vi) is acceptable if:~~

~~1) it includes all items relied on for safety in the identified accident sequences; and~~

~~2) the description of the items relied on for safety, their management measures, and the associated safety limits and margins is adequate to permit a determination of compliance with 10 CFR 70.62(c)(vi); and~~

~~3) information concerning the assignment of management measures to safety controls is adequate to show compliance with 10 CFR 70.62(d).~~

~~Acceptance criteria 1) through 3) above are explained in greater detail below.~~

~~1) ALL ITEMS: The primary function of the "list describing all items relied on for safety" is to document the safety basis of all processes in the facility to assist in assuring that these items~~

~~are not degraded or removed without a justifying safety review. Thus the key feature of this list is that every item relied on for safety be included. No item, aspect, feature, or property of the processes that is needed to show compliance with the safety performance requirements of the regulation may be left off this list.~~

~~For example, if a process upset is required before an accident may occur, and if, in showing compliance with 70.61 reliance is placed on the fact that this process upset is an unlikely event, then those features of the process that assure that the upset is of low frequency are an item relied on for safety. Similarly, if the dimension or the material composition of a piece of process equipment is essential to preventing an accident, then that dimension or material is an item relied on for safety. In such cases, only those dimensions, features, or properties of the process that are essential to the safety function are items relied on for safety. It is essential that such process features be clearly identified so that a description of their safety function is available to safety reviewers for change control.~~

~~Items relied on for safety include both hardware safety controls and administrative controls. All such items must be listed, no matter how low their safety significance, if they are relied on to demonstrate compliance with the safety performance requirements of 70.61. Such items may assure compliance by making the accident unlikely or by mitigating its consequences.~~

~~2) THE DESCRIPTIONS OF ITEMS: The essential features of each item relied on for safety (IROFS) that are required to achieve adequate reliability should be described. Sufficient information should be provided about hardware controls to permit an evaluation that, in principle, controls of this type will have adequate reliability. If the IROFS is an administrative control, 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.~~

~~3) MANAGEMENT MEASURES: The description of each item must contain any information needed to identify how the management measures, such as maintenance, training, configuration management, etc. of 10 CFR 70.62(d) 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. To show compliance with the performance requirements of 10 CFR 70.61, the description of the items relied on for safety and the management measures applied to them, must show how they meet all applicable provisions of the Baseline Design Criteria as described in Sections 4 through 7 and Section 11, or a lesser set of measures if justified. The primary justification for lesser management measures is lower risk significance.~~

~~One example of a tabular description of IROFS meeting these criteria is Table A-7 in Appendix A.~~

[Comment: The contents of paragraph 9 are deleted. Its substance has been condensed and listed as a "*license commitment*" described in §3.4.3.1(2).]

s acceptabl~~9.~~ if it

~~includes: management policies, organizational responsibilities, administrative controls, and procedures governing the performance, review, and approval of the initial ISA and any revisions to the ISA. The applicant commits to evaluating the need for updating the ISA to reflect changes using a team with similar qualifications to the team that originally prepared the ISA for the system under review. In addition, the applicant commits to maintain the ISA under an adequate configuration management function. The applicant also identifies updates to the table on controls necessary to ensure safety, as well as seeks prior approval for any changes that raise unreviewed safety questions or increase the level of~~

~~risk. Administrative controls ensure the independence of reviewing organizations and individual reviewers. The applicant establishes procedures to control records and supporting documentation concerning the ISA.~~

3.5 REVIEW PROCEDURES

3.5.1 Acceptance Review

The primary reviewer should ~~will~~ evaluate ~~review~~ the application to determine whether ~~if~~ it addresses the topics ~~contains the topics and information discussed~~ in Section 3.3, "Areas of Review." If significant deficiencies are identified ~~in the application~~, the applicant should ~~will~~ be requested to submit additional material ~~information~~ before the start of the safety evaluation. ~~The primary reviewer will then determine that the applicant has provided the information required. If necessary, a request for additional information to the applicant will be prepared in conjunction with the licensing project manager.~~[Comment: revise this paragraph to be consistent with the language used in comparable sections 3.5.1 of other SRP chapters.]

3.5.2 Safety Evaluation

[Comment: the text in each of the nine 'Safety Evaluation' topics should be simplified and made less repetitive of the 'Acceptance Criteria'. There is no need to repeat this information again. Simplicity of text is desirable!]

1. The staff reviews the applicant's license commitments pertaining to the ISA against the acceptance criteria described in §3.4.3.1. Of particular importance are commitments to maintaining the ISA current so as to serve as the facility's safety basis.

2~~1~~. The staff reviews the applicant's description of the site ~~facility~~ to ensure that all natural and man-made features and hazards that could impact facility safety have been identified. ~~determine if adequate information is presented to provide an understanding of those factors that could pose a hazard to the facility. The reviewer reviews the types, frequency, and severity of specific external hazards (such as locations of nearby airports, rail lines, port facilities, other nuclear or chemical facilities, dams, rivers, etc.) identified in the application. The reviewer similarly reviews natural external event hazards, such as severe weather conditions, hurricanes, earthquakes, floods, tornadoes, that are specific threats to the site.~~

3~~2~~. The staff reviews the applicant's description of the facility to ensure that the facility's building layout and location within the controlled area, distance from the site boundaries, and design information for protecting against external events have been adequately assessed. ~~to determine that the applicant has adequately discussed the features that could affect potential accidents and their consequences. The reviewer should verify that the applicant has provided information describing the location and arrangement of buildings at the site and their distance from the site boundary and nearby population. The reviewer should also determine that design criteria for the facility are justified on the basis that (1) they are sufficient to withstand the effects of credible external events that could occur at the site or (2) the consequences of such credible external events are acceptable, given their expected frequency of occurrence.~~

4~~3~~. The staff reviews the applicant's description of each process analyzed in the ISA to determine that it provides an adequate understanding of process function and theory, as well as major component function and operation. ~~The staff also reviews information provided on process design, equipment, and instrumentation to determine that it is sufficient to understand the results of the ISA.~~

~~4. The staff reviews the applicant's commitment to compile and maintain current and accurate process safety information on hazardous materials, process technology, and process equipment.~~ [Comment: this is referenced as a license commitment. Delete.]

5. The staff reviews the applicant's description of the ISA team to determine its ~~the~~ adequacy ~~of the makeup of the team and qualifications of the team leader and team members. The reviewer should determine that the qualifications of the team meet the acceptance criteria in Section 3.4.3.5.~~

6. The staff reviews the applicant's description of the selected ISA methodology ~~selected~~ to verify that it is acceptable for the proposed facility and its processes. ~~the applicant has cogently described the methodology (i.e., the methods used for hazard identification, hazard analysis and accident identification, accident consequence determination, and accident sequence evaluation)~~ and the bases for its choice. ~~The reviewer also verifies that the acceptance criteria in Section 3.4.3.6 are satisfied.~~

~~7. The staff reviews the narrative and tabular summary of the results of the ISA to determine if the information provided is complete and satisfies the acceptance criteria in Section 3.4.3.7 and Appendix A. The information reviewed includes:~~ [Comment: paragraph is incorrect and redundant. Delete.]

The staff reviews process-specific information including narrative descriptions of each process analyzed, hazards identified for each, initiating events, general types of accident sequences identified in the process hazards analysis and risk assessments for each.

~~a. a listing of hazardous materials and conditions and a table showing interactions between materials and between materials and conditions that could result in a hazardous situation; and~~

~~b. either:~~

~~(i) A tabular summary listing of each accident sequence that could result in radiological or chemical exposures to workers or the public, or environmental consequences. This tabular summary identifies for each sequence, the events that occur, including initiating event, and failures of safety controls, and the unmitigated consequences resulting. Staff reviews this list following the procedures in Appendix A; or, (ii) a set of logic diagrams that identify the all combinations and sequences of failure events that would cause consequences of concern.~~

8. The staff reviews the items relied on for safety for each general type of accident sequence. ~~tabular list describing the administrative and engineered safety controls identified in the accident sequences as being relied on for safety. The review determines if the controls satisfy the acceptance criteria provided in Section 3.4.3.8 and its appendix. These criteria specify the redundancy, independence, quality, and reliability of the controls needed to assure that the likelihood and consequences of identified accidents meet the safety performance requirements of 10 CFR 70.61.~~

~~The risk significance of accident sequences will be evaluated by staff using the risk indices from Table A-1 in Appendix A. The procedure for evaluating risk significance is described in the last section of Appendix A. Accident sequences will be placed in categories. Safety controls appearing in those sequences in the category of highest risk significance will each be reviewed in detail. Independent evaluation or site visits will be performed, if warranted. For accident sequences categorized as lower risk significance, staff will select a representative sample (e.g., 5 to 10%) of sequences for specific evaluation, while the remainder receive a less detailed review.~~ [Comment: this second paragraph of point 8 is unnecessarily prescriptive as it suggests that only the risk indices in Appendix A can be used. Appendix A – now recommended for relocation to NUREG-1513 – is simply an example and has no regulatory authority.]

9. The staff reviews the management measures ~~practices~~ applicable to each item relied on for safety to provide reasonable assurance that they will be reliable and available when required to perform their functions. ~~proposed by the applicant to ensure that the ISA is used so as to assure safety, and is kept current and accurate. The reviewer verifies that the applicant practices mandate adequate procedures for ISA performance, update, review responsibility, documentation, and record maintenance.~~

3.6 EVALUATION FINDINGS

The reviewer verifies that the applicant's license commitments and ISA Summary are ~~information submitted by the applicant~~ sufficiently complete so that compliance with 10 CFR Part 70 can be demonstrated ~~evaluated~~. The reviewer can document the evaluation of the commitments and ISA Summary as follows ~~also verifies that the applicant's submittal contains sufficient information and that the staff review supports statements and conclusions of the following type, which the staff should include~~ in the SER:

> Many hazards and potential accidents can result in unintended exposure of persons to radiation, radioactive materials, or toxic chemicals associated with licensed materials. The applicant has performed an Integrated Safety Analysis (ISA) to identify and evaluate those hazards and potential accidents, and to establish safety controls to ensure facility operation within the bounds of the ISA. The NRC staff has reviewed the ISA Summary and specifically those postulated accidents resulting from the facility hazards that may be anticipated to occur (or are considered unlikely or highly unlikely). To ensure that the performance criteria ~~limits~~ in 10 CFR Part 70 are met, the applicant has adequately established items relied on for safety ~~both administrative and engineered safety controls~~. The staff has reviewed these safety controls and applicable management measures and finds them acceptable based on the ISA Summary evaluation and other supporting information.
>
> The staff concludes that (1) the applicant has made acceptable commitments pertaining to the conduct and maintenance of an ISA, (2) that ~~identification and evaluation of the~~ hazards and accidents have been identified and evaluated as part of the ISA and (~~2~~3) that ~~the establishment of~~ controls have been established to maintain safe facility operation, to ~~from their consequences~~ meet the requirements of 10 CFR Part 70, and to provide reasonable assurance that the health and safety of the public will be adequately protected.

3.7 REFERENCES

AIChE, *Guidelines for Hazard Evaluation Procedures, Second Edition with Worked Examples*, American Institute of Chemical Engineers, New York, September 1992. [Comment: this reference is no longer cited in SRP Chapter 3. Delete it.]

American National Standards Institute, ANSI/ANS-8.1-1983, "Nuclear Criticality Safety in Operations With Fissionable Materials Outside Reactors," American Nuclear Society, La Grange Park, IL, 1983. [Comment: this reference is never cited in SRP Chapter 3. Delete it.]

American National Standards Institute, ANSI/ANS-51.1-1983, "Nuclear Safety Criteria for the Design of Stationary Pressurized Water Reactor Plants," American Nuclear Society, La Grange Park, IL, 1983. [Comment: this reference is never cited in SRP Chapter 3. Delete it.]

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

NUREG-1513, *Integrated Safety Analysis Guidance Document*, 1995.

U.S. Dept. of Commerce, Bureau of the Census, Statistical Abstract of the United States 1995, Table No. 688. [Comment: this reference is never cited in SRP Chapter 3. Delete it.]

~~APPENDIX A~~

~~EXAMPLE PROCEDURE FOR RISK EVALUATION~~

[Comment: Appendix A should be deleted from SRP Chapter 3. It provides guidance in the conduct of an ISA, rather than in the preparation of an ISA Summary, and therefore has no relevance for inclusion in NUREG-1530. Appendix A should be complemented with an Appendix B that outlines a qualitative approach for risk evaluation. Both Appendices should be relocated to NUREG-1513 ('*ISA Integrated Safety Analysis Guidance Document*') which will become the principal guidance document in the conduct of an ISA.]

PROPOSED REVISION OF SRP (NUREG-1520) CHAPTER 3
INCORPORATING THE RECOMMENDATIONS
OF THE
NUCLEAR ENERGY INSTITUTE
(AUGUST, 1999)

3.0 INTEGRATED SAFETY ANALYSIS (ISA) COMMITMENTS AND ISA SUMMARY

3.1 PURPOSE OF REVIEW

The purpose of this review is to establish reasonable assurance that the applicant or licensee will establish and maintain a safety program for the licensed facility that will satisfy the performance requirements of 10 CFR Part 70.61. A facility's safety program has three components: (i) maintenance of process safety information, (ii) performance and maintenance of an integrated safety analysis (ISA), and (iii) implementation of management measures that will ensure the availability and reliability, when required, of items relied on for safety identified in the ISA. The review conducted in Chapter 3 will address the first two components of the facility's safety program (process safety information, ISA). The third element of the safety program (management measures) will be assessed separately in Chapter 11 of this SRP.

The review is structured into two sections:

Section 1: Commitments	assessment of an applicant's commitments to undertake and maintain various analyses and databases, to implement corrective actions when safety-significant deficiencies are identified and to make informational reports to the NRC within specific timeframes
Section 2: ISA Summary	review of the ISA Summary to ensure identification of safety-significant external hazards and credible accident sequences whose consequences could exceed the performance criteria of 10 CFR 70.61, establishment of comparative risks, designation of appropriate items relied on for safety and implementation of acceptable management measures

Materials to be examined in the review include a list of license commitments pertaining to the ISA and the ISA Summary. The reviewer should understand that the applicant will have previously conducted an ISA, the results of which, including all supporting documentation (e.g. piping and instrumentation drawings (PI&Ds), dose calculations, drawings, ISA worksheets, criticality safety evaluations, etc.), will be maintained at the facility site. The ISA is not part of the license application and requires neither assessment nor approval by the reviewer. The applicant will also have prepared a summary of the ISA ('*ISA Summary*') that presents analyses of safety- and risk-significant issues identified at the facility. The ISA Summary is not part of the license application, but is submitted to the NRC for placement on the docket. Review of the ISA Summary is required to provide reasonable assurance to the reviewer that the applicant

has identified significant hazards at the facility, analyzed potential, credible accident sequences and implemented appropriate safety controls to prevent or mitigate such accidents. If deemed necessary, the reviewer may consult the ISA or background and supporting information not contained in the ISA Summary. For example, the reviewer may wish to review specific process criticality safety evaluations, the detailed results of an accident sequence analysis, the technical justification for selection of a particular risk classification method or the characteristics of a low-risk accident sequence not discussed in the ISA Summary.

3.2 RESPONSIBILITY FOR REVIEW

Primary: FCLB assigned reviewer

Secondary: Technical specialists in specific areas

Supporting: Fuel Facility Inspection Staff

3.3 AREAS OF REVIEW

The staff initially reviews the applicant's proposed license commitments pertaining to the ISA. This is followed by a detailed review of the ISA Summary.

3.3.1 License Commitments

Staff review of the applicant's safety program commences with examination of proposed license commitments. These commitments specifically pertain to the ISA and are in addition to other commitments the applicant will have made on other health and safety issues. This review must provide reasonable assurance that the applicant has committed to:

1. Compile and maintain current a database of process safety information that includes information pertaining to the hazards of materials used or produced in the process, information pertaining to the technology of the process and information pertaining to the equipment used in the process

2. Develop and implement procedures to keep the ISA and ISA Summary accurate and up-to-date. The applicant commits to maintaining the ISA as the facility's safety basis. The applicant commits to promptly analyzing and incorporating into the ISA any changes in the process safety information, operating procedures, process design bases, control systems or variables, instrumentation, items relied on for safety, management measures, etc., to revising the ISA, as required, and to submitting changes in the ISA Summary to the NRC in accordance with the schedule in 10 CFR 70.72(d)(1).

3. Address promptly any safety-significant process vulnerabilities or unacceptable performance deficiencies identified in the ISA

4. Design and implement a corrective action program to address any deviations from safe operating conditions (as defined in the SRP Glossary), accidents or other abnormal operational events that are encountered

5. Design and implement a facility change mechanism process whereby any proposed change to the process, operating procedures, flowsheet, items relied on for safety or their

management measures is first evaluated by the ISA methodology to establish its risk and safety-significance and to determine the need for a license amendment.

6. Engage suitably qualified and trained personnel to apply the ISA methodology, both in conducting the initial ISA and in performing updates when required

7. Maintain items relied on for safety for higher-risk accident sequences to ensure their reliability and availability when required

8. Implement an emergency preparedness program for use in the event an item relied on for safety or a management measure fails

9. Maintain a log at the facility that documents any item relied on for safety or management measure that failed to perform its function when required or when tested

3.3.2 ISA Summary

3.3.2.1 Purpose and Scope

The ISA Summary presents a succinct synopsis of the results of the ISA. The ISA Summary focuses on safety-significant features of a facility which could potentially pose the greatest risks to human health and safety and the environment. It presents a sub-set of the facility hazards and accident sequences analyzed in the ISA and tabulates both the items relied on for safety proposed by the applicant to prevent or mitigate such accidents and the management measures to ensure their reliability and availability when required.

The ISA Summary differs from the ISA in two substantive ways. The ISA Summary:

- discusses hazards and accident sequences at a *systems level* (*versus* at a component level in the ISA)
- focuses on high- and intermediate-consequence events that could exceed the performance requirements of 10 CFR Part 70.61 (*versus* consideration of *all* low- to high-risk accident sequences in the ISA)

The ISA Summary is intended to be a “stand-alone” document that succinctly distills from the ISA:

- ISA methodology
- ISA study team (members & qualifications)
- descriptions of facility processes, identification of process hazards and assessments of general types accident sequences
- risk classification approach for ranking general types of accident sequences
- high- and intermediate-risk accident sequences
- items relied on for safety for high- and intermediate-consequence events
- management measures applied to items relied on for safety

The level of technical and engineering detail in the ISA Summary is considerably less than in the ISA. For example, the ISA Summary requires descriptions of only the *general types* of credible accident sequences and not the detailed descriptions of each accident sequence assessed in the ISA. The ISA Summary relies more on *narrative text* and schematic flow

diagrams rather than on detailed technical information and data analysis. It should be structured to "walk" the primary reviewer through the plant's operations and individual processes. In doing so, the reviewer should be able to understand the principle of operation of the facility, recognize facility and process hazards, identify items relied on for safety to prevent or mitigate an accident and understand selection of management measures applied to such items relied on for safety. The reviewer should, as a result, be able to judge the adequacy of the applicant's safety program.

3.3.2.3 Format and Content

The ISA Summary should be structured into three sections and present the following information:

(i) General Information	information of a general nature applicable to all processes analyzed in the ISA, such as: • facility and site descriptions • ISA methodology(ies) • selection of appropriate exposure standards • ISA study team • definition of terms
(ii) Process-Specific Information	summary of risk and safety assessments of each facility process including: • processes analyzed • process hazards • general types of accident sequences • risk assessment of general types of accident sequences • items relied on for safety • management measures
(iii) Items Relied on For Safety	tabulations of items relied on for safety for safety-significant, general types of accident sequences

Information in the ISA Summary should primarily be excerpted from the ISA. Information that should be expected in each section of the ISA Summary is summarized below:

3.3.2.4 ISA Summary Review Topics

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

(i) General Information

1. The site description (see Section 1.3, "Site Description") concerning those factors that could affect safety, such as geography, meteorology (e.g., high winds and flood potential), seismology, and demography.

2. The facility description (see Section 1.1, "Facility and Process Description") concerning features that could affect potential accidents and their consequences. Examples of these features are facility location, facility design information, and the location and arrangement of buildings on the facility site.

3. The ISA study team that conducted the ISA, including the technical areas of expertise represented on the team and a description of the team's experience and qualifications in conducting ISAs.

4. The ISA method(s) used in conducting the ISA to identify hazards, forecast accident sequences and to predict their consequences and likelihoods of occurrence.

5. The definitions of terms used in performing the ISA, including those for the terms 'credible', 'unlikely', 'highly unlikely' and 'likely'

6. The quantitative standards used in the ISA to establish permissible acute exposures to licensed material or hazardous chemicals produced from licensed materials

(ii) Process-Specific Information

1. The tabulation of all processes analyzed in the ISA.

2. The safety assessment of each process. The process safety assessment will include the following components:

    a. process description (narrative description and a simple block flow diagram)

    b. hazard identification

    c. general types of accident sequences (identified in the ISA process hazard analysis)

    d. unmitigated consequences of each general type of accident sequence, their comparison to the performance requirements of 10 CFR Part 70.61(b) and (c) and their ranking in terms of risk.

    e. likelihood of occurrence of each general type of accident sequence

    f. risk classification of each general type of accident sequence

3. The description of items relied on for safety to prevent or mitigate each general type of accident sequence's risk to an acceptable level (so that the performance criteria of 10 CFR 70.61 are not exceeded), including classification by type (engineered or administrative controls) and, if applicable and explanation of how such items were graded according to their safety-importance.

4. The management measures applied to each item relied on for safety and, if applicable, a description of how such measures were graded

5. The compliance with the nuclear criticality monitoring requirements of 10 CFR 70.24

6. The description of how the design of new facilities or new processes at existing facilities adheres to the baseline design criteria of 10 CFR 70.64.

(iii) Items Relied on For Safety

1. The tabulation of all items relied on for safety that are required for each general type of accident sequence analyzed in the ISA, as well as any other safety controls or safeguards that the applicant has designated to be items relied on for safety

2. The tabulation of any item relied on for safety that is the sole item preventing or mitigating a general type of accident sequence that exceeds the performance requirements of 10 CFR Part 70.61

3.4 ACCEPTANCE CRITERIA

3.4.1 Regulatory Requirements

The requirement to describe the applicant's safety program, including both the ISA Summary and appropriate management measures, is specified in 10 CFR 70.65(a). The three components of the safety program are defined in 10 CFR 70.62(a). Licensee commitments to perform an Integrated Safety Analysis (ISA) using current process safety information and to keep the ISA updated and current as the facility's safety basis are specified in 10 CFR 70.62. 10 CFR 70.72 states requirements for keeping the ISA and its documentation current when changes are made to systems, structures, and components.

3.4.2 Regulatory Guidance

Guidance applicable to performing an ISA and documenting the results is contained in NUREG-1513, "Integrated Safety Analysis Guidance Document." A sample ISA Summary for one process is also available to illustrate an acceptable form and content.

3.4.3 Regulatory Acceptance Criteria

3.4.3.1 License Commitments

The staff will find an applicant's safety program commitments acceptable if the following criteria are met:

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

    a. the hazards of all materials used or produced in the process. Information on chemical and physical properties such as toxicity, acute exposure limits, reactivity, chemical and thermal stability such as is included on Material safety Data Sheets (meeting the requirements of 10 CFR 1910.1200(g)) should be provided.

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

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

2. The applicant commits to keeping the ISA and ISA Summary accurate and up-to-date by means of a suitable configuration management system. The ISA must account for any changes made to the facility or its processes (e.g. changes to the site, operating procedures, control systems). Management policies, organizational responsibilities, revision timeframe and procedures to perform and approve revisions to the ISA should be outlined succinctly. The applicant commits to evaluating any facility changes or changes in the process safety information that may alter the parameters of an accident sequence by means of the facility's ISA methodology. The applicant commits to using an ISA Team with similar qualifications to that used in conducting the original ISA for any modifications and revisions that the applicant deems necessary. The applicant commits to review of any facility changes that may increase the level of risk and, if dictated by revision of the ISA, to select and implement new or additional items relied on for safety and appropriate management measures. The applicant commits to submitting to the NRC revisions of the ISA Summary within the timeframe specified in 10 CFR 70.72(d)(1).

3. The applicant commits to promptly address any safety-significant vulnerabilities or unacceptable performance deficiencies identified in the ISA. Whenever an update of the ISA is conducted, the applicant commits to taking prompt and appropriate actions to address any vulnerabilities that may have been identified. If a proposed change results in a new type of accident sequence (e.g. different initiating event, significant changes in the consequences) or increases the risk of a previously analyzed accident sequence to an unacceptable level, the applicant commits to promptly evaluating the adequacy of existing items relied on for safety and associated management measures and to making necessary changes, if required.

4. The applicant commits to design and implement a corrective action program that will promptly address, implement and document appropriate responses to accidents, deviations from safe operating conditions and recommendations for process improvements. The program should be structured to address potential process vulnerabilities as well as actual accidents and incidents which have occurred. It should also be structured to respond to deficiencies identified in compliance audits. Facility policies to encourage the identification and reporting of process vulnerabilities (e.g. equipment malfunctions, problems with safety systems) or areas in which assurance of worker health and safety could be reasonably enhanced should be described. Procedures to describe internal evaluation of incidents should be described. The applicant should discuss the key components of the corrective action plan (e.g. investigative team, documentation of findings, implementation of corrective actions)

5. The applicant commits to design and implement a facility change mechanism that meets the requirements of 10 CFR 70.72. The applicant should discuss the key components of the written facility change mechanism such as: evaluation of the change within the ISA framework, prediction of impacts on worker health and safety, modifications to operating procedures, change authorization procedures, updating the facility ISA.

6. The applicant commits to engage personnel with appropriate experience and expertise in engineering and process operations to update and maintain current the ISA. The ISA team shall consist of individuals knowledgeable in the facility's ISA methodology and in process hazards analysis.

7. The applicant commits to installation of items relied on for safety (including administrative controls) and maintaining them in a functional state so that they are available and reliable when needed. Management measures (which are evaluated in SRP Chapter 11) comprise the principal mechanism by which the reliability and availability of items relied on for safety is assured.

8. The applicant commits to design and implement an emergency preparedness program for use in the event an item relied on for safety or management measure fails. The applicant's emergency preparedness program should outline emergency actions that employees are to perform in the event of a serious event (e.g. fire, unintentional release of licensed material or hazardous chemicals produced from licensed material, inadvertent nuclear criticality). The applicant's written emergency preparedness program should outline procedures to address, for example, pre-planning for emergency conditions, preparation of emergency plans, specification of employee actions in an emergency, worker evacuation, solicitation of off-site emergency response assistance.

9. The applicant commits to maintaining a log at the facility, in accordance with the requirement of 10 CFR 70.62(a)(3), that documents each discovery of an item relied on for safety or management measure that has failed to perform its function. The applicant commits to enter into the log following information such as: item relied on for safety or management measure that failed, affected safety functions, affected facility process(es), cause(s) of the failure, corrective or compensatory actio(s) taken.

3.4.3.2 ISA Summary

The staff will find an applicant's safety program description as presented in the ISA Summary to be acceptable if the following criteria are met:

(i) General Information

1. The description of the site is considered acceptable if the applicant includes or references the following information:

    a. A description of the site geography, including its location in relation to prominent natural and man-made features such as mountains, rivers, airports, population centersand possibly hazardous commercial and manufacturing facilities

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

    c. Characterization of natural phenomena (e.g., tornadoes, hurricanes, and earthquakes) and other external events sufficient to assess their impact on plant safety and to assess their likelihood of occurrence.

a. An appropriately-scaled plan map of the facility showing the 'controlled area' as defined in 10 CFR 20.1003 with supporting narrative text that explains how this area will be maintained and how activities of the public will be excluded or controlled.

The ISA Summary may reference information on the site contained in the ISA or submitted as part of the required data for SRP Chapter 1.3 ('*Site Description*').

2. The description of the facility is considered acceptable if the applicant includes or references the following information:

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

   b. Design information regarding the resistance of the facility to failures caused by credible external events, when those failures may produce consequences of concern.

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

The ISA Summary may reference information on the facility contained in the ISA or submitted as part of the required data for SRP Chapter 1.1 ('*Facility Description*'). The facility description is used to systematically evaluate the spatial relation between a process accident and the people and the environment that could be adversely affected. While there may be some duplication in the information included in the site description, the facility description should generally focus more on how plant structures and configurations may cause or impact the progression of an accident and how they may impact worker and public safety.

The siting and design of a facility may significantly impact the progression and outcome of an accident sequence in areas such as the following:

- number of workers potentially impacted
- off-site environmental impacts (e.g. proximity to rivers (unconfined spills or sizable leaks), nearby population centers, fires (ignitable reagents))
- airborne contamination (e.g. site topography and nearby terrain, predominant wind directions)
- extreme weather events (e.g. direct flooding, lightening and high winds, loss of power, loss of containment of waste holding ponds)
- on-site chemical storage (e.g. toxic release hazards (NH_3, Cl_2, UF_6, etc.), separation of caustics from acids and corrosives, storage tank separation distances (storage dikes, sumps, drains, waste, etc.))
- vehicle traffic flow patterns
- access and egress, evacuation routes, emergency exits (e.g. access for maintenance, sampling, repairs, access to hydrants, monitor and control valves)
- protection of piping and vessels from external impacts
- process piping corrosion protection (compatibility with corrosive acids)
- spill control (e.g. drainage directions and destinations, sumps, perimeter dikes, automated leak detection systems, treatment capacities)
- fire protection (e.g. ignition sources (transient and fixed), control of combustible materials and reagents, fire barriers, explosion hazards, appropriate fire fighting

equipment (CO_2, halon), shielding of water-based fire suppression systems adjacent to or in moderation controlled areas)
- personal protective equipment (e.g. locations of SCBA/airline respirators, safety showers and eyewash locations)
- spatial interactions

3. The description of the ISA team that prepared the ISA is considered acceptable if the following criteria are met:

   a. The ISA team leader is formally trained and knowledgeable in the ISA methodology and can demonstrate an adequate understanding of all process operations and hazards under evaluation.

   b. At least one member of the ISA team has thorough, specific, and detailed experience in each process that was evaluated

   c. Team members represent a variety of process operating and engineering design experience, in particular, radiation safety, nuclear safety, fire protection, and chemical safety disciplines.

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

The ISA Summary may reference information on the ISA Team that is contained in the ISA. The ISA Summary should highlight the technical areas of expertise represented on the team and include a description of the team's experience and qualifications in conducting ISAs.

4. The descriptive summary of the ISA methodology is considered acceptable if it describes the methods used for each ISA task, and the basis for selection of each method, so that the adequacy of the method is clear and appropriate according to the criteria described in NUREG-1513 for selection of ISA methods. The method used to perform the ISA must have adequately addressed the four ISA components: (i) hazard identification, (ii) process hazard analysis, including accident sequence construction and evaluation against the performance criteria of 10 CFR 70.61, (iii) specification of items relied on for safety, and (iv) recommendation of management measures. Staff will find the ISA methodology acceptable if the following criteria are met:

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

      i. Incorporated the process safety information for the facility, and specifically, information pertaining to the hazards of licensed material and other hazardous chemicals used or produced by the process, the technology of the process (e.g. process chemistry, safe limits for operating parameters, consequences of process deviations) and equipment used in the process (e.g. PI&Ds, ventilation system design, safety systems, etc.). ISA methods may include, for example, "*Hazard and Operability Analysis (HAZOP)", "What If Analysis," "Fault Tree Analysis," "Preliminary Hazards Analysis*" or a combination of one or more of such approaches. Any commercial software packages used in the analysis should be identified. Finally, if the ISA was performed in accordance with specific industry standard or with one endorsed by a professional organization (e.g. American Institute of Chemical Engineers), these standards should be identified.

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

i. Considered credible external factors (e.g. meteorological, seismological, hydrological) as initiators of accident sequences that could pose a threat to facility workers, the public or the environment

b. The selected process hazard analysis method is considered acceptable if:

i. Its selection was consistent with the guidance provided in NUREG-1513

ii. It adequately addressed all the hazards identified in the hazard identification task of section 4.a above. The applicant identifies and justifies any hazards eliminated from further consideration.

i. The applicant has provided acceptable qualitative or quantitative definitions of terms used in evaluating the likelihood of occurrence of an accident sequence (e.g. 'likely', 'unlikely', 'highly unlikely') and in defining what constitutes a 'credible accident sequence'). The definition for 'credible' will likely incorporate some reference to the likelihood of the accident occurring. In general, a 'credible' accident is one that has some non-negligible probability of occurrence during the reference timeframe. An accident sequence may be characterized as 'credible' if there is an upset condition associated with the process that can reasonably be expected to occur. For example, exceeding concentration or mass limits or violating favorable geometry parameters (bottle volumes) or violating spacing limits are all credible upset conditions that could lead to an inadvertent nuclear criticality incident. Such an accident sequence would be deemed 'credible.' An 'incredible' event, in contrast, has a likelihood of occurrence approximating zero during the reference timeframe.

iv. It provides reasonable assurance that the applicant identifies significant types of accident sequences (including the items relied on for safety used to prevent or mitigate the accidents) that could exceed the performance criteria identified in §70.61.

v. It takes into account the interactions of identified hazards and proposed items relied on for safety, including system interactions, to ensure that the overall level of risk at the facility is consistent with the requirements of §70.61 and appropriately limited.

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

n assessing ge eral

types of accident sequences. Appropriate qualitative or quantitative methods have been used to forecast both the likelihood and consequences of each type of accident sequence. The applicant also states which quantitative acute exposure standards were used for hazardous chemicals. Nuclear criticality consequences may have been estimated through use of standard American Nuclear Society or equivalent standard methods. Environmental, industrial and chemical consequences, including fire and explosion, may have been estimated with the assistance of material safety data sheets, chemical interaction information and computer modeling techniques including emission calculations and air dispersion models. Each type of unmitigated accident sequence is compared to

the performance criteria of 10 CFR 70.61 and should any fall into the high- or intermediate-consequence event categories, the applicant has recommended appropriate items relied on for safety. A ranking of the general types of accident sequence *by risk* should be included in the application.

d. The applicant demonstrates that an effective method was used to provide reasonable assurance that the recommended administrative or engineered safety controls (items relied on for safety) will ensure that the risk of any accident sequence will not exceed the performance criteria of 10 CFR 70.61.

e. The applicant used acceptable quantitative standards to establish permissible acute exposures to licensed materials or hazardous chemicals produced from licensed materials. The chosen acute exposure standards should be identified and a brief, supporting explanation provided supporting the selection. Numerical acute exposure limits for those principal chemical compounds analyzed in the ISA accident sequences (e.g. HNO_3, UF_6, HF, etc.) should be tabulated. Any chemical compounds for which an Alternate Concentration Limit (ACL) was used in the ISA should be identified and a brief explanation substantiating its use provided.

(ii) Process-Specific Information

1. The facility process tabulation is acceptable if all processes analyzed in the ISA are properly identified and referenced to the facility description.

2. The safety assessment of each process is acceptable if the following information is provided:

    - a narrative description of the process that is sufficiently detailed to enable the reviewer to understand the process' theory of operation. This description should provide an overview of the basic process function, major process components (e.g. mixing, sintering, neutralization), process inputs and outputs (e.g. reagents, licensed material forms, products, wastes) and an explanation of how the process integrates with other facility process operations. This information, which should be summarized from the ISA, may be supported with process schematics, simple block flow diagrams, chemical flow sheets or tables of information. A brief statement of the safety basis(es) of the process as applicable to each of the generic hazards should be included. For example, in discussing a general type of accident sequence that could result in an inadvertent nuclear criticality, parameters that are controlled (e.g. geometry, concentration, mass, etc.) should be specified and credible accident sequences associated with the process (e.g. exceeding concentration or mass limits, violating favorable geometric parameters or bottle spacings, etc.) should be stated. The description should limit the amount of quantitative information.
    - identification of all hazards for the process resulting from process deviations (e.g. volume, concentration, temperature), initiating events internal to the facility (e.g. fire) and credible external events (e.g. floods, hurricanes). Hazards of particular interest are those listed in 10 CFR 70.65(b)(3): radiological, chemical and facility hazards
    - a list of general types of accident sequences identified in the process hazard analysis. Brief narrative text should explain each generic accident type, including the initiating event(s). Note that specific accident sequences should not be listed.

General types of accident sequences for different initiating hazards may include, for example:

Initiating Hazard Type	General Type of Accident Sequence
Radiological	"loss of moderation control due to water ingress" "radiological exposure of workers to airborne uranium"
Chemical	"breakage of a control valve on a UF6 cylinder resulting in an inadvertent release of uranium hexafluoride"
Facility	"worker injury caused by moving parts in pug mills" "ignition of hydraulic lubricating oils"

- specification of the unmitigated consequences of each general type of accident sequence, linkage to the initiating event(s)
- likelihood of occurrence of each general type of accident sequence. The likelihood may be expressed in either a qualitative or quantitative manner based on the method used in conducting the ISA
- risk classification of each general type of accident sequence. Risk is computed to be the product of the consequence and the likelihood forecast for the general type of accident. The comparative risk of the general type of accident sequence is established through comparison against the performance criteria of 10 CFR 70.61

3. The description of the items relied on for safety is acceptable if the applicant:

- identifies which general types of accident sequence require items relied on for safety to reduce their risk to acceptable levels. High consequence events forecast to be highly unlikely or intermediate consequence events forecast to be unlikely do not require application of any items relied on for safety. Similarly, no items relied on for safety are required for general types of accident sequences that are neither high- or intermediate-consequence events.
- enumerates *at the systems level* appropriate items relied on for safety that, when applied to a general type of accident sequence, will provide reasonable assurance that the performance requirements of 10 CFR 70.61 will be met. Selection of appropriate items relied on for safety will depend upon the safety bases and parameters that are used to control a process.
- classifies each items relied on for safety as one of the following:

  (1) administrative control: operation requires human intervention for operation (e.g. oversight of sampling program, maintenance of logs of SNM, sealing of drums, timing of addition of reagents, visual inspection of leaks)

  (2) augmented administrative control: administrative control that relies on a warning device to notify an operator that intervention is necessary to implement a control (e.g. solution level alarm)

  (3) active engineered control: controls that use active sensors and that require no operator intervention to operate (e.g. in-line concentration monitors, automatic valve closures, tank level controls or automatic shut-off valves, solution pH controller)

  (4) passive engineered control: controls that use only fixed design features and that require no operator intervention to operate (e.g. compatibility of materials of construction with solutions, dikes and

secondary containment pits, deadman valves, multiple evacuation routes, storage of flammable liquids in NFPA-approved storage cabinets)

- explains how the item relied on for safety will prevent or mitigate an accident sequence
- explains how any items relied on for safety were graded according to their safety importance in accordance with 10 CFR 70.62(a)

4. The description of management measures is acceptable if the applicant:

    - proposes suitable management measures for item(s) relied on for safety for each general type of accident sequence so as to provide continuing assurance of compliance with the requirements of 10 CFR 70.61
    - briefly describes the management measures applied to each generic type of accident sequence and classifies each as active engineered, passive engineered, administrative or augmented administrative
    - explains how the management measure will provide reasonable assurance that the items relied on for safety will be reliable and available to perform its safety function, when required
    - explains how management measures were graded according to the reduction of risk attributable to a particular safety control or control system in accordance with 10 CFR 70.62(d)

5. The description of methods to comply with the nuclear criticality monitoring requirements of 10 CFR 70.24 is acceptable if the applicant:

    - provides a narrative description of the criticality monitoring system and information that demonstrates its capability to detect the minimum radiation levels in 109 CFR 20.24(a)
    - provides a suitably-scaled plan drawing of the location of criticality detectors and alarms relative to process operations in which accident sequences potentially leading to inadvertent nuclear criticalities were identified in the ISA

6. The description of how the design of a new facility or of a new process at an existing facility (including proposed items relied on for safety) adheres to the baseline design criteria of 10 CFR 70.64 is acceptable if the applicant:

    - outlines how compliance with the ten criteria listed in 10 CFR 70.64(a) has been established:
        (a) quality assurance and records: explanation of how management measures were selected to ensue that items relied on for safety will be reliable and available when required to perform their function and commitments to retain records on the performance and maintenance of such management measures
        (b) natural phenomena hazards: protection against external, natural hazards at a level equivalent to the most severe, documented historical event at the facility (e.g. floods, hurricanes, winds)
        (c) fire protection: protection against fires and explosions
        (d) environmental and dynamic effects: protection against environmental conditions; protection from dynamic events associated with normal

facility operations (e.g. operation, maintenance, testing) and postulated, credible accidents

(e) chemical protection: protection against chemical risks produced from licensed material, plant conditions that affect the safety of licensed material and hazardous chemicals produced from licensed material

(f) emergency capability: design features to maintain control of licensed material, to ensure the safe evacuation of on-site personnel and the availability of both on-site and off-site emergency services and facilities (e.g. hospitals, fire prevention)

(g) utility services: provision of emergency utility services when required

(h) management measures: inspection, testing and maintenance programs for items relied on for safety

(i) nuclear criticality controls

(j) instrumentation and controls: for monitoring and controlling the behavior of items relied on for safety

- demonstrates adherence to defense-in-depth design practices including a preference for engineered controls over administrative controls and implementation of procedures that limit challenges to items relied on for safety

(iii) Items Relied on For Safety

1. The tabulations of items relied on for safety required by 10 CFR 70.65(b) are acceptable if the applicant provides for each general type of accident sequence:

- list of all items relied on for safety. This list should include the following information in an abbreviated form:
  - (i) information on the administrative or engineered control (e.g. nature of the expected operator response, description of the piece of safety equipment) that is applied to each general type of accident sequence
  - (ii) information on the management measures applied to the item relied on for safety and any safety grading thereof
  - (iii) if applicable, information showing compliance of the item relied on for safety with the baseline design criteria of 10 CFR 70.64(a)
- list of items relied on for safety that are the sole item preventing or mitigating an accident sequence that could exceed the performance requirements of 10 CFR 70.61

3.5 REVIEW PROCEDURES

3.5.1 Acceptance Review

The primary reviewer should evaluate the application to determine whether it addresses the topics in Section 3.3, “Areas of Review.” If significant deficiencies are identified, the applicant should be requested to submit additional material before the start of the safety evaluation.

3.5.2 Safety Evaluation

1. The staff reviews the applicant's license commitments pertaining to the ISA against the acceptance criteria described in §3.4.3.1. Of particular importance are commitments to maintaining the ISA current so as to serve as the facility's safety basis.

2. The staff reviews the applicant's description of the site to ensure that all natural and man-made features and hazards that could impact facility safety have been identified.

3. The staff reviews the applicant's description of the facility to ensure that the facility's building layout and location within the controlled area, distance from the site boundaries, and design information for protecting against external events have been adequately assessed.

4. The staff reviews the applicant's description of each process analyzed in the ISA to determine that it provides an adequate understanding of process function and theory, as well as major component function and operation.

5. The staff reviews the applicant's description of the ISA team to determine its adequacy

6. The staff reviews the applicant's description of the selected ISA methodology to verify that it is acceptable for the proposed facility and its processes. and the bases for its choice..

7. The staff reviews process-specific information including narrative descriptions of each process analyzed, hazards identified for each, initiating events, general types of accident sequences identified in the process hazards analysis and risk assessments for each.

8. The staff reviews the items relied on for safety for each general type of accident sequence

9. The staff reviews the management measures applicable to each item relied on for safety to provide reasonable assurance that they will be reliable and available when required to perform their functions.

3.6 EVALUATION FINDINGS

The reviewer verifies that the applicant's license commitments and ISA Summary are sufficiently complete so that compliance with 10 CFR Part 70 can be demonstrated. The reviewer can document the evaluation of the commitments and ISA Summary as follows: in the SER:

> Many hazards and potential accidents can result in unintended exposure of persons to radiation, radioactive materials, or toxic chemicals associated with licensed materials. The applicant has performed an Integrated Safety Analysis (ISA) to identify and evaluate those hazards and potential accidents, and to establish safety controls to ensure facility operation within the bounds of the ISA. The NRC staff has reviewed the ISA Summary and specifically those postulated accidents resulting from the facility hazards that may be anticipated to occur (or are considered unlikely or highly unlikely). To ensure that the performance criteria in 10 CFR Part 70 are met, the applicant has adequately established items relied on for safety. The staff has reviewed these safety

controls and applicable management measures and finds them acceptable based on the ISA Summary evaluation and other supporting information.

The staff concludes that (1) the applicant has made acceptable commitments pertaining to the conduct and maintenance of an ISA, (2) that hazards and accidents have been identified and evaluated as part of the ISA and (3) that controls have been established to maintain safe facility operation, to meet the requirements of 10 CFR Part 70, and to provide reasonable assurance that the health and safety of the public will be adequately protected.

3.7 REFERENCES

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

NUREG-1513, *Integrated Safety Analysis Guidance Document*, 1995.