



DCS-NRC-000249
30 September 2009

U.S. Nuclear Regulatory Commission
ATTN: Document Control Desk
Washington, DC 20555

SUBJECT: Docket No. 070-03098
Shaw AREVA MOX Services
Responses to a Request for Additional Information Regarding the
Integrated Safety Analysis Methodology Described in the License
Application and Integrated Safety Analysis Summary

REFERENCE: 1. Letter from Kevin Morrissey to Dealis Gwyn dated March 25,
2009 entitled "Request for Additional Information Regarding the
Integrated Safety Analysis Methodology Described in the License
Application and Integrated Safety Analysis Summary for the
Mixed Oxide Fuel Fabrication Facility"

Shaw AREVA MOX Services hereby responds to the Request for Additional Information (RAI) contained in Reference 1. Our responses to the RAIs are contained in the enclosure. The License Application and Integrated Safety Analysis Summary, which include the associated changes, will be transmitted under separate cover.

If you have any questions, please contact Dealis Gwyn, Licensing and Regulatory Compliance Manager, at (803) 819-2780.

Sincerely,

A handwritten signature in black ink, appearing to read "D Stinson". The signature is stylized with a large, looped initial "D" and a horizontal line extending to the right.

David Stinson
President and COO

11/15/09
11/15/09

DCS-NRC-000249

30 September 2009

Page 2

Attachment: Response to Request for Additional Information Regarding the Integrated Safety Analysis Methodology Described in the License Application and Integrated Safety Analysis Summary for the Mixed Oxide Fuel Fabrication Facility

cc: (w/ attachment)

David Tiktinsky, USNRC/HQ

EDMS: Corresp\Outgoing\NRC\2009 NRC\DCS-NRC-000249

cc: (w/o attachment)

Eric Chassard, MOX Services

Mostafa Dayani, NNSA/SRS

Carol R. Elliott, NNSA/SRS

Walter Elliott, MOX Services

Sam Glenn, NNSA/SRS

William Gloersen, USNRC/RII

Dealis Gwyn, MOX Services

William Hennessy, MOX Services

Kevin Morrissey, USNRC/HQ

Deborah Seymour, USNRC/RII

Donald Silverman, Esq., ML&B LLP

DCS-NRC-000249
Attachment
30 September 2009

Attachment

Response to Request for Additional Information Regarding the Integrated Safety Analysis Methodology Described in the License Application and Integrated Safety Analysis Summary for the Mixed Oxide Fuel Fabrication Facility

**MOX Fuel Fabrication Facility Responses to
Integrated Safety Analysis Methodology Requests for Additional Information**

ISA-LA-1

The LA states in Section 5.1.2 that “Mixed Oxide (MOX) uses personnel with appropriate experience and expertise in engineering and process operations to perform the Integrated Safety Analysis (ISA). For revisions to the ISA, personnel having qualifications similar to those ISA team members performing the ISA are used, depending on the nature of the changes.” How the terms “appropriate,” “similar,” and “nature” will be evaluated is not well defined. The requirements for qualification need to be referenced or included in the LA. The term “similar” needs to be more clearly described so that the experience and expertise requirements are understood. The nature of the changes needs to be expanded upon so that it is clear how and when this commitment will be implemented.

This information is needed to comply with § 70.22(a)(6). This regulation requires that each application for a license shall contain the technical qualifications, including training and experience of the applicant and members of his staff to engage in the proposed activities in accordance with the regulations.

Reply:

The last paragraph of Section 5.1.2 is deleted. ISA team qualifications are described in Section 5.3. Revised Section 5.3 to clarify the responsibilities and qualifications for ISA team leader and members. See reply to ISA-LA-19 for details.

ISA-LA-2

In Section 5.1.3, a commitment is made to implement and maintain management measures. However, it is not clear how management measures will be applied (implemented) to specific items relied on for safety (IROFS) to assure their reliability and availability. It is also not clear how management measures will be maintained and what criteria will be used for maintaining them. Provide a discussion, or table, that shows how management measures will be applied to IROFS and will be maintained.

This information is needed to comply with § 70.62(d). This regulation requires that each applicant or licensee shall establish management measures to ensure compliance with the performance requirements of § 70.61.

Reply:

Section 5.1.3 has been revised to add a pointer to Section 5.2.5.2.4 where application of management measures is discussed.

ISA-LA-3

In Section 5.1.4, commitments are made regarding making changes to the ISA Summary and LA. Included in this section are statements about making changes to the LA that would not require the U.S. Nuclear Regulatory Commission (NRC) pre-approval of the changes. The commitment to make changes to the LA without NRC pre-approval should include: (1) the criteria for evaluating the need for pre-approval including the impact on safety and health, (2) requirements for documenting and maintaining the evaluation, and (3) a time frame when the changes not requiring NRC pre-approval will be provided to the NRC.

This information is needed to comply with § 70.9(a). This regulation requires that information provided to the Commission by an applicant for a license or by a licensee, or information required by statute or by the Commission's regulations, orders, or license conditions to be maintained by the applicant or the licensee and be complete and accurate in all material respects.

Reply:

References to changing the LA in accordance with § 70.72 have been removed from Section 5.1.4. Chapter 16 has been created to discuss how MOX Services will evaluate potential changes to the LA. The discussion in Chapter 16 regarding making changes to the LA without NRC pre-approval includes (1) the criteria for evaluating the need for pre-approval including the impact on safety and health, (2) requirements for documenting and maintaining the evaluation, and (3) a time frame when the changes not requiring NRC pre-approval will be provided to the NRC.

ISA-LA-4

In Section 5.1.4, reference is made to member companies and affiliates for the purpose of evaluating new processes under § 70.72(c)(1)(ii). Provide clear definition for member companies and affiliates by providing a list of applicable member companies and affiliates or a discussion of the criteria used to determine the qualifying companies.

This information is needed to demonstrate compliance with § 70.72. This regulation allows the licensee to make changes to the site, structures, processes, systems, equipment, components, computer programs, and activities of personnel, without prior Commission approval, if the change does not use new processes, technologies, or control systems for which the licensee has no prior experience.

Reply:

Reference to member companies and affiliates has been removed from Section 5.1.4.

ISA-LA-5

The requirement in § 70.72(e) contains a timeliness component (promptly) that is not included in your commitment made in Section 5.1.4. The staff considers that the timeliness component is an integral part of the regulation and for consistency and clarity should be included in the LA.

This information is needed to demonstrate compliance with § 70.72(e). This regulation requires that if a change covered by § 70.72 is made, the affected on-site documentation must be updated promptly.

Reply:

The sentence in Section 5.1.4 pertaining to § 70.72(e) has been revised to include the timeliness component (promptly).

ISA-LA-6

In Section 5.1.4, a commitment is made regarding changes that require NRC pre-approval. Reference to an undefined group is provided for submitting amendment requests to the NRC. It is not clear from this commitment the relationship between the responsible group and the responsibility to submit amendment requests. Modify or clarify the statement.

This information is needed to demonstrate compliance with § 70.72(d)(3). This regulation requires that for changes that require pre-approval under § 70.72, the licensee shall submit an amendment request to the NRC in accordance with § 70.34 and § 70.65 of this chapter, and for all changes that affect the ISA Summary, the licensee shall submit to the NRC annually, within 30 days after the end of the calendar year during which the changes occurred, revised ISA Summary pages.

Reply:

Section 5.1.4 has been clarified to indicate that MOX Services will submit amendment requests.

ISA-LA-7

The requirement in § 70.62(a)(3) contains a timeliness component (promptly) regarding the updating of records with regard to failure of IROFS that is not included in your commitment made in Section 5.1.5. The staff considers that the timeliness component is an integral part of the regulation and for consistency and clarity should be included in the LA.

This information is needed to demonstrate compliance with § 70.72(e). This regulation requires that if a change covered by § 70.72 is made, the affected on-site documentation must be updated promptly.

Reply:

The sentence in Section 5.1.5 pertaining to § 70.72(e) has been revised to include the timeliness component (promptly).

ISA-LA-8

In Section 5.2, in describing the ISA methods, is there a criterion for evaluating the consequences and likelihoods? If so, reference to the criteria should be included in the discussion of the methods used.

This information is needed to demonstrate compliance with § 70.62(a). This regulation requires that each licensee or applicant establish and maintain a safety program that demonstrates compliance with the performance requirements of § 70.61.

Reply:

The performance requirements of 10 CFR §70.61 provide the criteria used to evaluate event consequence and likelihood. The introductory text of Section 5.2 discusses the determination of event consequence and likelihood for potential events. This section also discusses the selection of IROFS to ensure the performance requirements of 10 CFR §70.61 are satisfied.

Consequence and likelihood evaluations are described in Section 5.2.4, 5.2.5, and 5.2.6.

ISA-LA-9

In Section 5.2 and Table 5.1-2 reference is made to a “typical” risk matrix. It is not clear what typical means in these instances and whether other matrices exist or will be used. Clarify or modify the term to be consistent with implementation of the matrix.

This information is needed to demonstrate compliance with § 70.62(d). This regulation requires that each applicant or licensee establish management measures to ensure compliance with the performance requirements of § 70.61.

Reply:

The risk matrix discussed in Section 5.2 and shown in Table 5.1.2 will be used by MOX Services to determine risk. The term “typical,” as used to describe risk matrices, is removed from LA text.

ISA-LA-10

In Section 5.2.2, in describing subtasks of the safety evaluations, the identification and

description of IROFS does not include how management measures are applied to IROFS. Is the application of management measures to IROFS considered part of the ISA method? If so, it should be included in the ISA methods discussion in the LA.

This information is needed to comply with § 70.62(d). This regulation requires that each applicant or licensee shall establish management measures to ensure compliance with the performance requirements of § 70.61.

Reply:

Section 5.2.2 is an introductory section. The application of management measures is considered to be part of the ISA method and is discussed in Section 5.2.5.2.4.

ISA-LA-11

In Section 5.2.2, it is not clear what “design verification activities” refer to and the commitment that is being made regarding the design verification process. Provide a description of what these activities are and what activities are being committed to.

This information is needed to demonstrate compliance with § 70.62(a). This regulation requires that each licensee or applicant establish and maintain a safety program that demonstrates compliance with the performance requirements of § 70.61.

Reply:

“Design verification activities” refers to a MFFF QA process that requires a review of design output, ensuring that the design meets the specified design input and conforms to other specified requirements. Requirements for the performance of design verification are included in the MOX Project Quality Assurance Plan (MPQAP), specifically Design Control. Revised Section 5.2.2 to remove the term “design verification activities” since all IROFS are subject to the requirements of the MPQAP as discussed in Chapter 15.

ISA-LA-12

In Section 5.2.2.1, it is not clear what constitutes the commitments for the methodology that will be performed versus what is a description of the methodology that was applied in the past. This is complicated by the use of both past and present tense verbs. Confirm what commitments relate to the methodology that will be used if a license is granted and what portions of the methodology represent either description only or historical documentation.

A review of the methodology description should be performed to sort out the historical, descriptive and commitment aspects of the ISA method that will apply to a possession and use license so that a clear understanding of the ISA method that is being committed to and that will be used in the future can be evaluated by the staff.

This information is needed to demonstrate compliance with § 70.62(a). This regulation requires that each licensee or applicant establish and maintain a safety program that demonstrates compliance with the performance requirements of § 70.61.

Reply:

Revised Chapter 5 to remove discussion of the Safety Analysis of Design Basis (SA) and to limit discussion to those aspects of the ISA that apply to the MFFF possession and use phase. Corrected tense accordingly.

ISA-LA-13

In Section 5.2.2.1, provide the basis for selecting the appropriate process hazards analysis (PrHA) method.

This information is needed to demonstrate compliance with § 70.62(a). This regulation requires that each licensee or applicant establish and maintain a safety program that demonstrates compliance with the performance requirements of § 70.61.

Reply:

The specific PrHA methodologies utilized for each process unit are selected using the guidance of *Guidelines for Hazard Evaluation Procedures – Second Edition – With Worked Examples*, Center for Chemical Process Safety, American Institute of Chemical Engineers, New York, NY, 1992 and *Integrated Safety Analysis Guidance Document*, NUREG-1513, U.S. Nuclear Regulatory Commission, 1999.

Revised Section 5.2.2 to clarify the basis used for selecting PrHA methods and any supplemental methods that may be used in the evaluation of MFFF hazards.

ISA-LA-14

In Section 5.2.2.5, the criteria for “not credible” for natural phenomena and external man-made events is satisfied because of an extremely low initiating event frequency. Quantify what corresponds to extremely low for these particular events. Also provide the acceptance criteria for other events that are based on frequency of occurrence of an initiating event.

This information is needed to demonstrate compliance with § 70.62(a). This regulation requires that each licensee or applicant establish and maintain a safety program that demonstrates compliance with the performance requirements of § 70.61. This information is also needed to demonstrate compliance with § 70.64(a)(2). This regulation requires that the design must provide for adequate protection against natural phenomena with consideration of the most severe documented historical events for the site.

Reply:

An extremely low initiating frequency is generally accepted to be a frequency of occurrence of less than once in a million years. NUREG-1520 defines "not credible" as "an external event for which the frequency of occurrence can conservatively be estimated as less than once in a million years." This criterion was used to eliminate natural phenomena hazards and external man-made hazards as discussed in the applicable screening evaluations performed by MOX Services. This specific criterion is not applied to MFFF process events.

Revised Section 5.2.5, Likelihood Evaluation, to define extremely low initiating event frequency. Revised definition of "Not Credible" as follows:

Natural phenomena or external man-made events with an extremely low initiating event frequency, conservatively estimated as less than once in a million years.

ISA-LA-15

In Section 5.2.2.7, what are the criteria for determining which of the PrHA methods is used to demonstrate the likelihood of an event?

This information is needed to demonstrate compliance with § 70.62(a). This regulation requires that each licensee or applicant establish and maintain a safety program that demonstrates compliance with the performance requirements of § 70.61.

Reply:

The method used for the evaluation of event likelihood is developed from guidance provided in NUREG-1513 and NUREG-1718. The method is qualitative and provides reasonable assurance that high-consequence events are highly unlikely and intermediate-consequence events are unlikely.

Supplemental analyses may be performed to support likelihood determinations obtained with the qualitative method. These analyses provide insight into event likelihoods, event sequences, single failure vulnerability and other safety aspects of hazards evaluation and may include such techniques as Failure Modes and Effects Analysis (FMEA), Fault Tree Analysis and Event Tree Analysis. Selection and performance of these techniques are based upon the specific application and the guidance of the following documents:

- Guidelines for Hazard Evaluation Procedures – Second Edition – With Worked Examples, Center for Chemical Process Safety, American Institute of Chemical Engineers, New York, NY, 1992 and,
- Integrated Safety Analysis Guidance Document, NUREG-1513, U.S. Nuclear Regulatory Commission, 1999.

Likelihood definitions and the criteria that ensure reliability of the selected IROFS are provided in Section 5.2.5.

ISA-LA-16

In Section 5.2.2.7, a statement is made that implementation of management measures cannot be performed because the procedures are not available. Commit to implement management measures when procedures are available or justify why implementation is not necessary.

This information is needed to demonstrate compliance with § 70.62(a). This regulation requires that each licensee or applicant establish and maintain a safety program that demonstrates compliance with the performance requirements of § 70.61. This information is also needed to comply with § 70.62(d). This regulation requires that each applicant or licensee shall establish management measures to ensure compliance with the performance requirements of § 70.61.

Reply:

Section 5.2.2.7 paragraph discussing management measure implementation is removed as a result of resolving ISA-LA-12. Commitment to implement management measures is discussed in Section 5.1.3. Implementation of management measures is discussed in Section 5.2.5.2.

ISA-LA-17

In Section 5.2.2.7.1, the statement is made that a summary is provided in the Nuclear Safety Evaluations (NSEs) that includes how the performance requirements are met with the application of the identified IROFS. Provide this information in the ISA summary.

This information is needed to demonstrate compliance with § 70.62(a). This regulation requires that each licensee or applicant establish and maintain a safety program that demonstrates compliance with the performance requirements of § 70.61.

Reply:

Event evaluation summary tables in the ISA Summary provide this information. See for example, Table 5.3.3-4, Summary of Loss of Confinement Event Evaluation. These tables provide the following information: Events, Receptor, IROFS, Sole IROFS status, and additional protective features.

ISA-LA-18

In Section 5.2.2.7.1, the statement is made that the demonstration that the single failure criterion is applied to each IROFS is in the NSEs. How does this apply to sole IROFS?

This information is needed to demonstrate compliance with § 70.62(a). This regulation requires that each licensee or applicant establish and maintain a safety program that demonstrates compliance with the performance requirements of § 70.61.

Reply:

In the event that a sole IROFS is credited, a "sole IROFS" justification is provided. This may include a discussion of additional management measures (e.g., increased surveillance frequencies), fail-safe characteristics, highly reliable components, or the application of non-credited additional protection features.

Section 5.2.5.2.1 has been revised to clarify the justification of sole IROFS.

ISA-LA-19

In Section 5.5, what specific criteria apply to ISA Team qualification in terms of knowledge, experience, MOX-specific experience and education? What are the training or re-training requirements associated with ISA Team qualifications?

This information is needed to comply with § 70.22(a)(6). This regulation requires that each application for a license shall contain the technical qualifications, including training and experience of the applicant and members of his staff to engage in the proposed activities in accordance with the regulations.

Reply:

Process Hazards Analyses (What-If/Checklist, HAZOP) are performed by a team of reviewers referred to as the ISA team. The ISA team consists of four basic participants: 1) team leader, 2) team scribe, 3) process or responsible engineer, and 4) discipline experts. The team leader provides direction for the team to ensure a thorough evaluation. The team scribe documents the discussions of the team during the evaluation. The responsible engineer provides detailed knowledge of process unit equipment and operations. Discipline experts provide input concerning the various design disciplines involved in the process and may include:

- Radiochemical process
- Chemical processes (i.e., aqueous polishing)
- Civil/structural/geotechnical
- HVAC
- Glovebox design
- Nuclear criticality safety
- Electrical
- Fire protection
- Instrumentation and control
- Mechanical
- MOX fuel process
- Operations

- Radiation protection
- Nuclear safety
- Human factors engineering

Discipline experts are selected based on the process and associated hazards. Discipline experts may attend portions of the hazard evaluations or be placed on call based on the discretion of the team leader.

ISA team member responsibilities and qualification are listed below:

ISA Team Leader The team leader is responsible for providing direction for the performance of the ISA hazard evaluation and ensuring the evaluation is conducted in an efficient and thorough manner. The team leader ensures that all materials and resources (i.e., drawings, support analyses, design descriptions, meeting rooms, etc) required to perform the hazard evaluation are available. The ISA team leader is responsible for selecting the appropriate Discipline Experts for the process being evaluated. The ISA Team leader shall have a good working knowledge of the process being evaluated. The ISA team leader shall be knowledgeable and experienced in the method chosen for performance of the ISA hazard evaluation. This requirement may be satisfied by formal training in the specific methodology or one (1) year experience performing the specific hazard evaluation methodology. The ISA team leader shall not be the responsible engineer for the process being evaluated.

Team Scribe The team scribe is responsible for documenting the discussions that take place during performance of the hazard evaluation. Documentation is performed in a format dictated by the hazard evaluation method. The team scribe shall be familiar with the method chosen for performing the ISA hazard evaluation and the process unit being evaluated. The team scribe performs his duties under the direction of the Team Leader.

Responsible Engineer The responsible engineer is an experienced team member with detailed knowledge of the process unit being evaluated. The responsible engineer provides information concerning process unit design, as well as the associated technology and theory of operation.

Discipline Expert The discipline expert is an experienced team member with knowledge of a specific design discipline. The discipline expert provides the team with information used to identify and evaluate events, as well as determine applicable mitigative/preventive controls.

Section 5.5 has been revised to include the above description of the ISA team member responsibilities and qualifications.

ISA-LA-20

In Figure 5.2-2, the method shows a step that the frequency of the event crediting the IROFS will be determined. Define the term "frequency." Explain whether this step is part of the ISA methodology described in that section.

This information is needed to demonstrate compliance with § 70.62(a). This regulation requires that each licensee or applicant establish and maintain a safety program that demonstrates compliance with the performance requirements of § 70.61.

Reply:

Deleted LA Chapter 5 figures in response to ISA-LA-12. Evaluation of likelihood is discussed in Section 5.2.5.

Additional questions from radiological review that pertain to Chapter 5 of the LA

ISA-LA-RAD-1

Section 5.3.1.2, top of page 5.3.1-3, indicates the ISA evaluates credible events for four separate areas which are facility worker, site worker, individual outside the Mixed Oxide Fuel Fabrication controlled area (IOC), and the environment. However, Section 5.3.2, second full paragraph on page 5.3.2-1, only lists three of these four. In the following paragraph, all four areas are again listed. Consistent with 10 CFR 70.62(c), confirm that the evaluation described in the second full paragraph of Section 5.3.2 was conducted on all the groups of concern.

Also, in Section 5.3.2 third paragraph, second sentence states, “the unmitigated event consequences have been determined to be low to the site worker, facility worker, the IOC, and the environment.” As currently written, this sentence states that all unmitigated event consequences have been determined to be low. The intent of this paragraph is to indicate that some of the unmitigated event consequences were determined to be low and thus no IROFS were assigned. However, the current text is unclear, since 5.3.3 through 5.3.11 contains unmitigated events which have high and intermediate consequences. Consistent with 10 CFR 70.62(c), add additional information to the third paragraph of Section 5.3.2 to clarify which unmitigated event consequences are being referenced. In addition the third sentence in paragraph three begins with, “these events....” Clarify to which events the sentence refers.

Reply (Part 1):

The ISA evaluates credible events for the facility worker, site worker, IOC, and the environment. The consequences for site worker, IOC and environment are determined by calculation (quantitative determination). Facility worker consequences are qualitatively determined based on the material released, the release mechanism, and the location of the worker relative to the release. In most cases, events involving an airborne release of plutonium or americium are judged to have high consequences to the facility worker and IROFS are applied. However, threshold values of MAR below which facility worker exposures exceeding 25 rem are not possible are used to categorize some events as low. The second paragraph of Section 5.3.2 only discusses quantitatively determined consequences.

ISA Summary, Section 5.3.2, second paragraph has been revised to add a sentence describing the qualitative determination of facility worker dose. Qualitative evaluation of facility worker dose is described in LA Section 5.2.3.2.

Reply (Part 2):

The intent of the paragraph is to state that credible events posing unmitigated low consequence do not require the identification of IROFS. Paragraph has been revised to clarify.

ISA-LA-RAD-2

Section 5.1.2.3.5, the first sentence of the second full paragraph states, "to perform the mitigated consequence analysis, the unmitigated consequence analysis methodology was used with the following modification: applicable bounding leak path factors (LPFs) were used for the IROFS providing mitigation." The section goes on to provide a single example of an LPF being modified due to a ventilation IROFS. As stated in Section 5.1.2.3.5, the IROFS effectiveness to mitigate high and intermediate consequence events is directly related to the accuracy of the assigned LPF. Yet, the LPF value for each IROFS has not been provided, nor the method used to ensure accuracy of the chosen value. Consistent with 10 CFR 70.61(e) and 70.62(c)vi, list the IROFS which have mitigative effects in whole or part due to reduced LPF values. List the LPF value for these IROFS and provide a basis for the accuracy of the assigned value.

Reply:

Only two LPF values are used in the dose calculations supporting the ISA Summary. An LPF value of 1.0 is used to evaluate event unmitigated consequences, events for which filtration is ineffective (i.e., gas releases), and events for which no filtration is credited. An LPF value of 1.0 models the release of all airborne material.

Mitigated consequences are calculated using an LPF of 1×10^{-4} . As stated in the ISA Summary, the applicable bounding values for the LPF are established in NUREG/CR-6410, Section 3.2.2.5 and Table F-6. The undamaged tested final high efficiency particulate air (HEPA) filter units with the upstream filter elements are normally expected to provide an overall LPF of approximately $10 \text{ E-}8$ or better. The ISA conservatively credits a LPF of $10 \text{ E-}4$ to allow for uncertainties. This is based on two filter banks in series.

ISAS Section 5.1.2.3.5 has been revised to explicitly state LPFs used in the ISAS and the supporting bases.

LA Sections 5.2.3.4, *Quantitative Mitigated Consequence Analysis*, and 5.2.3.1.1, *Source Term Evaluation*, have been revised to clarify the use of LPFs in consequence evaluation methodology.

Questions based on the ISA Summary

ISA-ISAS-1

How will the IROFS boundaries be defined, controlled and maintained for determinations of IROFS failures, ability of the IROFS to perform their safety functions, and for assigning and determining the effectiveness of management measures?

This information is needed to comply with § 70.65(b)(4). This regulation requires that the ISA summary must contain information that demonstrates compliance with the performance requirements of § 70.61, including a description of the management measures.

Reply:

IROFS boundaries are defined by the IROFS assigned safety function. All associated components, including support systems, required to perform the assigned safety function are identified as IROFS. IROFS boundaries are maintained and controlled through MFFF Nuclear Safety Evaluations (NSE) and Nuclear Criticality Safety Evaluations (NCSE). These documents identify IROFS and safety functions at a group level (e.g., glovebox) in the event evaluations. Detailed listings of the associated component identifiers (e.g., NDP*GB1000) are provided in table form in the document body or attachments to the NSE/NCSE. The NSE/NCSEs are prepared and maintained in accordance with the design and records management controls of the MPQAP.

LA Section 5.2.6 has been revised to discuss the definition, control and maintenance of IROFS boundaries.

ISA-ISAS-2

How are IROFS failures, or operability, defined? Define a time period for evaluation of whether an IROFS is no longer capable of performing its safety function. Describe the process for implementing compensatory measures for failed IROFS.

This information is needed to comply with § 70.62(a)(3). This regulation requires that each licensee or applicant shall maintain records of failures readily retrievable and available for NRC inspection, documenting each discovery that an IROFS or management measure has failed to perform its function upon demand or has degraded such that the performance requirements of § 70.61 are not satisfied. These records must identify the IROFS or management measure that failed and the safety function affected, the date of discovery, date (or estimated date) of the failure, duration (or estimated duration) of the time that the item was unable to perform its function, any other affected IROFS or management measures and their safety function, affected processes, cause of the failure, whether the failure was in the context of the performance requirements or upon demand or both, and any corrective or compensatory action that was taken. A failure must be recorded at the time of discovery and the record of that failure updated promptly upon the conclusion of each failure investigation of an IROFS or management measure.

Reply:

Definitions of IROFS operability are defined in the MFFF Operating Limits Manual (OLM). The MFFF OLM defines operational modes, operability requirements, limiting conditions for operation and associated completion times, and required surveillances and frequencies.

LA Section 5.2.5.3 has been revised to include a discussion of the OLM.

ISA-ISAS-3

Given that your methodology considers the entire set of IROFS when determining compliance with the 70.61 performance requirements, what is the process for determining whether replacement of an IROFS is equivalent?

This information is needed to demonstrate compliance with § 70.72(c)(2). This regulation requires that the licensee does not remove, without at least an equivalent replacement of the safety function, an IROFS that is listed in the ISA Summary and is necessary for compliance with the performance requirements of § 70.61.

Reply:

The process to evaluate IROFS replacement shall determine IROFS equivalency such that the performance criteria of 10 CFR 70.61 are satisfied. The existing IROFS safety function, IROFS type (engineered/administrative, passive/active), and the facility events for which the item is credited will be identified. Ability of the replacement IROFS to perform the required safety function with an equivalent reliability will be verified. The following four criteria are applied:

- Application of Single Failure Criteria,
- Application of Industry Codes and Standards,
- Application of the MPQAP, and
- Application of Management Measures.

The process will be implemented by approved facility procedures as part of the configuration management program. A discussion of change control is provided in LA Section 15.2.6, Change Control.

ISA-ISAS-4

Are the criteria for meeting highly unlikely defined by your methodology the same for sole IROFS as they are for other IROFS?

This information is needed to comply with § 70.65(b)(4). This regulation requires that the ISA summary contain information that demonstrates compliance with the performance requirements of § 70.61.

Reply:

In cases where a single active system, component or activity of personnel is the sole IROFS preventing or mitigating an accident sequence that exceeds the performance requirements of 10 CFR § 70.61, justification is provided to demonstrate that it is designed to perform its safety function. This may include a discussion of additional management measures (e.g., increased surveillance frequencies), fail-safe characteristics, highly reliable components, or the application of non-credited additional protection features.

Discussion of single failure criterion is provided in LA Section 5.2.5.2.1.

ISA-ISAS-5

What is the relationship between performance of the supplemental likelihood assessments and demonstration of performance requirements? Are these assessments expected to be part of the methodology for evaluating future changes?

This information is needed to comply with § 70.65(b)(4). This regulation requires that the ISA summary contain information that demonstrates compliance with the performance requirements of § 70.61.

Reply:

While HAZOP and What-If/Checklist are the main techniques used to evaluate MFFF events, supplemental hazard evaluations may be performed in specific instances to support the ISA. These supplemental analyses are performed to gain insight into event likelihoods, event sequences, single failure vulnerability and other safety aspects of hazards evaluation and may include such techniques as Preliminary Hazards Analysis, Failure Modes and Effects Analysis (FMEA), Fault Tree Analysis and Event Tree Analysis. Selection of these techniques are based upon the specific application and the guidance of the following documents:

- Guidelines for Hazard Evaluation Procedures – Second Edition – With Worked Examples, Center for Chemical Process Safety, American Institute of Chemical Engineers, New York, NY, 1992 and,
- Integrated Safety Analysis Guidance Document, NUREG-1513, U.S. Nuclear Regulatory Commission, 1999.

LA Section 5.2.2 has been revised to address supplemental hazards analyses.

ISA-ISAS-6

A large number of the accident sequences in the ISA summary have conclusions that events are highly unlikely because of a partial set of the four elements used in your methodology for meeting the criteria of highly unlikely. It is not clear if only the elements provided in the conclusion are met or whether all four of the criteria required by your methodology have been met. Examples of this can be found on pages 5.3.3-8, 5.3.3-9b, 5.3.3-11 and 5.3.3-13. In cases where the full complement of elements defined for

acceptability are not met, justification for making an exception to the methodology is required or revision to the ISA Summary is needed for consistency with the results of the ISA.

This information is needed to comply with § 70.65(b)(4). This regulation requires that the integrated safety analysis summary must contain information that demonstrates the licensee's compliance with the performance requirements of § 70.61.

Reply:

Where applicable, the following four criteria are applied to all IROFS:

- Application of Single Failure Criteria,
- Application of Industry Codes and Standards,
- Application of the MPQAP, and
- Application of Management Measures.

A small number of sole IROFS and robust passive IROFS are credited in the evaluation of MFFF events. In these cases, the single failure criterion is not applicable as discussed in reply to ISA-ISAS-4. Also, codes and standards are generally not applied to administrative controls. ISA Summary risk conclusions have been revised to clarify the application four criteria listed above.

ISA-ISAS-7

Provide a discussion on how common mode failure is evaluated in the ISA methodology. Also provide a description of how independence is evaluated in the methodology when determining that the single failure criteria are acceptable for meeting the performance requirements.

This information is needed to comply with § 70.65(b)(4). This regulation requires that the ISA summary must contain information that demonstrates the licensee's compliance with the performance requirements of § 70.61.

Reply:

Common mode failure is addressed during performance of process hazards analysis, the identification of IROFS, and application of the single failure criterion. Multiple failures resulting from a single occurrence are considered to be a single failure (also referred to as a common mode or common cause failure).

The following hierarchy of controls is established regarding the application of IROFS with respect to the single failure criterion:

- Protection by a single passive safety device
- Protection by independent and redundant active-engineered features
- Protection by a single hardware system/engineered feature
- Protection by enhanced administrative controls

- Protection by simple administrative controls.

To ensure adequate implementation of the single failure criterion, the following principles are applied to the design of IROFS:

- Redundant equipment or systems – A piece of equipment or a system is redundant if it duplicates the operation of another piece of equipment or system to the extent that either may perform the required function (either identically or similarly), regardless of the state of operation or failure of the other.
- Diversity – Equipment or systems may satisfy single-failure criterion by providing diverse means of performing an IROFS safety function. This diverse means of performing the safety function is by equipment that does not duplicate the operation of another piece of equipment (redundancy), but still achieves the reliability required for the safety function. Each diverse system (means, paths, trains, etc.) or component is not required to provide for additional redundancy.
- Independence – IROFS are designed to ensure that the effects of natural phenomena and of normal operating, maintenance, testing, and postulated accident conditions on redundant equipment or systems do not result in the loss of their safety function, or are demonstrated to be acceptable on some other defined basis.
- Separation – IROFS are separated to the extent that failure of a single system component, or failure or removal from service of any IROFS that is common to the other systems and the IROFS leaves intact an IROFS satisfying applicable reliability, redundancy, and independence requirements.
- Fail-safe – IROFS are designed to fail into a safe state or into some other non-threatening defined basis if conditions such as disconnection of a system, loss of energy, or loss of pressure occur.

These design principles are implemented through the application of applicable codes and standards. Discussion of common mode failure is provided in LA Section 5.2.5.2.1.