

MFFFNPEm Resource

From: Kevin Morrissey
Sent: Thursday, February 12, 2009 1:14 PM
To: DWGwyn@moxproject.com
Cc: MFFFHearingFile Resource
Subject: FW: Draft RAI's for the I&C and Electrical Engineering Review
Attachments: Electrical RAIs.doc; Instrumentation and Controls RAIs.doc

Attached are a preliminary list of questions in the areas of I&C and Electrical Engineering for discussion with your staff in Rockviile on 2/25/09.

It is expected that some of these questions will be used as is or are the basis for the development of additional questions to be used for a formal RAI transmittal to you for the purpose of docketing your responses to complete the I&C and Electrical Engineering reviews. The questions pertain to the review of the MOX License Application and ISA Summary.

Hearing Identifier: MixedOxideFuelFabricationFacility_NonPublic
Email Number: 1366

Mail Envelope Properties (3DF2506A7257014AAC5857E5E852DEAC052DE0D6DE)

Subject: FW: Draft RAI's for the I&C and Electrical Engineering Review
Sent Date: 2/12/2009 1:13:38 PM
Received Date: 2/12/2009 1:13:40 PM
From: Kevin Morrissey

Created By: Kevin.Morrissey@nrc.gov

Recipients:

"MFFFHearingFile Resource" <MFFFHearingFile.Resource@nrc.gov>
Tracking Status: None
"DWGwyn@moxproject.com" <DWGwyn@moxproject.com>
Tracking Status: None

Post Office: HQCLSTR02.nrc.gov

Files	Size	Date & Time
MESSAGE	530	2/12/2009 1:13:40 PM
Electrical RAIs.doc	76794	
Instrumentation and Controls RAIs.doc		120314

Options

Priority: Standard
Return Notification: No
Reply Requested: No
Sensitivity: Normal
Expiration Date:
Recipients Received:

**Mixed Oxide Fuel Fabrication Facility—Licensing Review
Request for Additional Information
Plant Systems – Electrical Design**

PS-E-1

ISA Section 5.3.9.2.2

Specify the bounding parameters used to identify and define the external man-made hazard EMMH-03, Loss of Offsite Power, in terms of expected maximum frequency of occurrence and anticipated maximum duration of the event.

10CFR 70.62 (c)(1)(iv) requires that each applicant conduct and maintain an integrated safety analysis that identifies potential accident sequences caused by process deviations or other events internal to the facility and credible external events, including natural phenomena. 10 CFR 70.62 (c)(1)(v) requires that each applicant conduct and maintain an integrated safety analysis that identifies the consequences and likelihoods of occurrence of each potential accident sequence identified pursuant to paragraph (c)(1)(iv) and the methods used to determine the consequences and likelihoods. This information is needed to support an evaluation of whether the IROFS required to mitigate this event will be adequately reliable.

PS-E-2

ISA Section 5.3.9.2.2

Provide a description of how the evaluation of the Loss of Offsite Power event accounts for an assessment of historical and anticipated future occurrences of off-site grid-reliability related, and onsite electrical equipment reliability related outages, or other postulated reliability-related causes, in addition to the Natural Phenomena Hazards (NPH) identified in Section 5.3.8 of the ISA. Alternatively, provide a demonstration of how the frequency of occurrence and the expected duration of such grid reliability-related outages are bounded by the analysis of the natural phenomena evaluated.

10CFR 70.62 (c)(1)(iv) requires that each applicant conduct and maintain an integrated safety analysis that identifies potential accident sequences caused by process deviations or other events internal to the facility and credible external events, including natural phenomena. 10 CFR 70.62 (c)(1)(v) requires that each applicant conduct and maintain an integrated safety analysis that identifies the consequences and likelihoods of occurrence of each potential accident sequence identified pursuant to paragraph (c)(1)(iv) and the methods used to determine the consequences and likelihoods. This information is needed to support an evaluation of whether the IROFS will be adequately reliable.

Enclosure 1

PS-E-3

ISA Sections 1.1.7 and ISA Section 5.3

For the hazards and accident sequences evaluated in the ISA that require electrical power for IROFS to operate to mitigate such events, identify the maximum allowable time for each event sequence which may be safely tolerated immediately following a Loss of Offsite power, before emergency power must be restored.

10CFR 70.62 (c)(1)(iv) requires that each applicant conduct and maintain an integrated safety analysis that identifies potential accident sequences caused by process deviations or other events internal to the facility and credible external events, including natural phenomena. 10 CFR 70.62 (c)(1)(v) requires that each applicant conduct and maintain an integrated safety analysis that identifies the consequences and likelihoods of occurrence of each potential accident sequence identified pursuant to paragraph (c)(1)(iv) and the methods used to determine the consequences and likelihoods. 10 CFR 70.64 (a)(7) requires that the design of new facilities must provide for continued operation of essential utility services. This information is needed to support an evaluation of whether the IROFS will be adequately reliable.

PS-E-4

ISA Sections 1.1.7 and ISA Section 5.3, LA Sections 11.4.1.1.2 and 11.4.1.1.3

For the hazards and accident sequences evaluated in the ISA that require electrical power for IROFS to operate to mitigate such events, identify the criteria for determining the magnitude of the minimum delay time required before re-application of power for IROFS needed to mitigate each event sequence to allow for the decay of electro-magnetic fields to prevent damage to continuously running electrical motors. For the protection of this function, state whether hard-wired interlocks will be used to avoid connection of out-of-phase sources.

10 CFR 70.64 (a)(7) requires that the design of new facilities must provide for continued operation of essential utility services.

10 CFR 70.61 (e) requires each engineered or administrative control or control system necessary to comply with paragraphs (b), (c), or (d) of Section 70.61 shall be designated as an item relied on for safety, and that the safety program shall ensure that each item relied on for safety will be available and reliable to perform its intended function when needed and in the context of the performance requirements of section 70.61.

10 CFR 70.64 (a)(4) requires that the design of new facilities must provide for adequate protection from environmental conditions and dynamic effects associated with normal operations, maintenance, testing, and postulated accidents that could lead to loss of safety functions.

PS-E-5

LA Section 11.4.1.1.3 pages 11.4-7 and 11.4-8

Confirm or clarify the apparent statement that during the restoration mode, the non-IROFS PLCs are programmed to synchronize both offsite incoming feeders with the two (restored) standby generators (assuming both are available) supplying the MFFF electrical system. Provide an explanation as to the reason why it is necessary for each bus of emergency loads to transfer to a different (respective) off-site feeder source, or whether this process is necessary to restore normal power via a closed transition (i.e., make-before-break) process.

NUREG 1718 Section 5.4.3.2.B.xi states: "The applicant describes the essential features of each IROFS that are required to achieve adequate reliability. The applicant should provide sufficient information about engineered hardware controls to permit an evaluation that, in principle, [demonstrates that] controls of this type will have adequate reliability.

PS-E-6

LA Section 11.4.1.2.2, page 11.4-8

Clarify whether it will be necessary to control the electrical system in the event of a 480 VAC service failure that lasts beyond the 125 VDC battery one-hour capacity time, and if so, what are the provisions for doing so.

NUREG 1718 Section 5.4.3.2.B.xi states: "The applicant describes the essential features of each IROFS that are required to achieve adequate reliability. The applicant should provide sufficient information about engineered hardware controls to permit an evaluation that, in principle, [demonstrates that] controls of this type will have adequate reliability.

PS-E-7

LA Section 11.4.2.2 Pages 11.4-10, and 11.4-7

Clarify the description of the standby generator starting process. The current description states that the standby generators are capable of accepting load (i.e., are at rated speed and voltage) within 10 seconds to sustain all IROFS loads, life-safety loads, and loads important for facility production. However following a loss of offsite power, the standby power mode may not be initiated until it has been determined that voltage is not available on both normal buses for a period of 5 seconds to allow time for a transfer from one incoming feeder to the other. This is an apparent non-compliance with the requirements for life safety loads (NFPA-101, IEEE-446, etc.) which require a 10-second maximum power restoration time from the onset of a loss of power condition.

NUREG 1718 Section 5.4.3.2.B.xi states: "The applicant describes the essential features of each IROFS that are required to achieve adequate reliability. The applicant should provide sufficient information about engineered hardware controls to permit an evaluation that, in principle, [demonstrates that] controls of this type will have adequate reliability.

PS-E-8

ISA Sections 4.4.1, 4.4.2, and 4.4.3 and LA Section 11.4.1

Provide an analysis that demonstrates that the total time it takes to restore power (loss of power detection, bus transfer time, non-essential load shedding, and time for the emergency diesel generator to attain running speed and voltage and be connected to/synchronized to the bus) to the IROFS loads following a loss of offsite power is considered adequate for accomplishing the mitigation functions needed for the worst-case event sequence (i.e., event requiring electrical utility restoration in the shortest amount of time.) Alternatively, provide a statement and an analysis that demonstrates that all IROFS loads requiring immediate restoration of electrical power or continuous electrical power to accomplish safety functions are connected to buses that are backed by a qualified uninterruptible power supply.

10 CFR 70.64 (a)(7) requires that the design of new facilities must provide for continued operation of essential utility services. 10 CFR 70.62 (c)(1)(vi)) requires that each applicant conduct and maintain an integrated safety analysis that identifies each item relied on for safety, the characteristics of its preventative, mitigative, or other safety function, and the assumptions and conditions under which the item is relied upon to support compliance with the performance requirements of Section 70.61. NUREG 1718 Section 5.4.3.1.D states that the applicant's methodology for applying likelihoods to the accidents examined...should "address any design bases that ensure that the principal SSC will function as intended (e.g., safety margins for criticality)." This information is needed to support an evaluation of whether the IROFS will be adequately reliable.

PS-E-9

ISA Sections 4.4.1, 4.4.2, and 4.4.3 and LA Section 11.4.1

Provide an analysis that demonstrates that the capacities of the emergency AC and DC power systems are adequate to accomplish all IROFS load power supply requirements for the duration of the maximum anticipated loss of power event identified in the response to question PS-E-1 above or until normal power can otherwise be restored. For example, justify why a one-hour operational requirement is considered adequate for the design of the emergency DC power supply batteries.

10 CFR 70.64 (a)(7) requires that the design of new facilities must provide for continued operation of essential utility services. 10 CFR 70.62 (c)(1)(vi)) requires that each applicant conduct and maintain an integrated safety analysis that identifies each item relied on for safety, the characteristics of its preventative, mitigative, or other safety function, and the assumptions and conditions under which the item is relied upon to support compliance with the performance requirements of Section 70.61. NUREG 1718 Section 5.4.3.1.D states that the applicant's methodology for applying likelihoods to the accidents examined...should "address any design bases that ensure that the principal SSC will function as intended (e.g., safety margins for criticality)." This information is needed to support an evaluation of whether the IROFS will be adequately reliable.

PS-E-10

ISA Section 4.4.3.1.3 and LA Section 11.4

Identify the criteria for designing the emergency power load application sequence. Identify the criteria for determining which loads are to be automatically placed onto the bus and which are to be manually connected, and what factors contribute to the decision for applying loads manually.

10 CFR 70.64 (a)(7) requires that the design of new facilities must provide for continued operation of essential utility services. 10 CFR 70.62 (c)(1)(vi) requires that each applicant conduct and maintain an integrated safety analysis that identifies each item relied on for safety, the characteristics of its preventative, mitigative, or other safety function, and the assumptions and conditions under which the item is relied upon to support compliance with the performance requirements of Section 70.61. NUREG 1718 Section 5.3.2 states that the ISA Summary should contain a description of "IROFS for all accidents in each process sufficiently to understand their safety function in meeting the appropriate consequence and likelihood requirements of 10 CFR 70.61," as well as the "information... demonstrating compliance with baseline design criteria required by 10 CFR 70.64(a)(1) through (5) and (7) through (10) for new facilities...and required to be submitted in accordance with 10 CFR 70.65 (b)(4). Since these elements all bear on the adequacy of IROFS, it is efficient to include their review in the ISA Summary review." This information is needed to support an evaluation of whether the IROFS will be adequately reliable.

PS-E-11

ISA Sections 4.4.2.2 and 4.4.3.1.2

Provide the criteria for determining the sizing requirements for the standby and emergency diesel generator diesel oil storage tanks in a manner that envelopes the expected event sequences and frequency and duration of loss of offsite power conditions, plus allows for anticipated contingencies. Clarify the statement regarding the sizing of the standby generator fuel oil storage tank. Clarify whether the statement that the storage tank is sized to provide for a storage capacity for "each standby generator" to function for 24 hours at 100% load is meant to indicate that it is sized to provide a storage capacity that allows for both standby generators to operate at 100% load continuously for 24 hours, or only one standby diesel generator to operate for 24 hours at 100% load.

10 CFR 70.64 (a)(7) requires that the design of new facilities must provide for continued operation of essential utility services. NUREG 1718 Section 5.4.3.2.B.iii states that an acceptable ISA meets the following criteria for a description of facility processes:

- "(c) Process design and equipment, including a discussion of the process design, equipment, and instrumentation that is sufficiently detailed to permit an adequate understanding of the results of the ISA."

PS-E-12

LA Section 11.4 and ISA Sections 4.4.1, 4.4.2, and 4.4.3

Provide a clear statement in the description in the License Application and the ISA Summary as to whether the active engineered electrical control devices used to detect loss of voltage, undervoltage, overcurrent, or under and over-frequency, etc., conditions needed to control the breakers and start and connect the emergency diesel generators that apply and maintain emergency power to critical plant IROFS are identified individually and treated as IROFS, designated as QL-1 components, and included within listings of IROFS components to which the quality management measures apply.

10 CFR 70.64 (a)(7) requires that the design of new facilities must provide for continued operation of essential utility services. 10 CFR 70.61 (e) requires each engineered or administrative control or control system necessary to comply with paragraphs (b), (c), or (d) of Section 70.61 shall be designated as an item relied on for safety, and that the safety program shall ensure that each item relied on for safety will be available and reliable to perform its intended function when needed and in the context of the performance requirements of section 70.61.

10 CFR 70.64 (a)(10) requires that the design of new facilities provide for the inclusion of instrumentation and control systems to monitor and control the behavior of items relied on for safety.

10 CFR 70.65 (b)(6) requires that the integrated safety analysis summary must contain a list briefly describing each item relied on for safety in sufficient detail to understand the functions in relation to the performance requirements of Section 70.61.

10 CFR 70.62 (d) requires that management measures shall be established to ensure compliance with the performance requirements of Section 70.61. The management measures shall ensure that engineered and administrative controls and control systems that are identified as items relied on for safety are designed, implemented, and maintained, as necessary, to ensure that they are available and reliable to perform their function when needed, to comply with the performance requirements of Section 70.61.

NUREG 1718 Section 15.3.1 states that the safety controls should be identified by the ISA Summary (discussed in Chapter 5.0 of this SRP). Individual components and support systems for the safety controls may have to be individually maintained to ensure the availability and reliability of the control function.

NUREG 1718 Section 5.3.2 states that the ISA Summary should contain a description of "IROFS for all accidents in each process sufficiently to understand their safety function in meeting the appropriate consequence and likelihood requirements of 10 CFR 70.61," as well as the "information... demonstrating compliance with baseline design criteria required by 10 CFR 70.64(a)(1) through (5) and (7) through (10) for new facilities...and required to be submitted in accordance with 10 CFR 70.65 (b)(4). Since these elements all bear on the adequacy of IROFS, it is efficient to include their review in the ISA Summary review."

PS-E-13

LA Section 11.4 (Bottom of page 11.4-1 to top of page 11.4-2) and Section 11.4.5

Resolve an apparent conflict regarding the definition of adequate acceptance criteria for the grounding system resistance to earth. On page 11.4-2 the applicant states that the MFFF grounding system complies with the requirements of NFPA 70, "and certain other applicable grounding codes and standards." NFPA 70 does not specify an acceptable maximum resistance to earth ground, but rather indicates that if the resistance of a grounding rod, pipe, or plate has a resistance exceeding 25 ohms, additional rods, pipes, or plates must be added in parallel to it. LA Section 11.4.5 indicates that IEEE Standard 142, "Recommended Practice for Grounding of Industrial and Commercial Power Systems," 1991 will be used to define criteria for IROFS. IEEE 142-1991 indicates that "adequate values" for connection to earth ground should have resistance in the one-to-five ohm range, and that the value of 25 ohms in the NEC's NFPA 70 code should not be interpreted as "satisfactory level for a grounding system." State definitively which standard is being used to identify design acceptance criteria for maximum resistance to earth for the MFFF grounding system.

10 CFR 70.64 (a)(4) requires that the design of new facilities must provide for adequate protection from environmental conditions and dynamic effects associated with normal operations, maintenance, testing, and postulated accidents that could lead to loss of safety functions.

PS-E-14

LA Section 11.4.1.1.2, page 11.4-3 and Figure 11.4-1, page 11.4-25

Verify that the 4000 Amp circuit breakers connecting the 15/20/25 MVA station service transformers to the two trains of 4160 VAC normal switchgear via rigid, metal-enclosed, copper transition buses are commercially available from nuclear qualified vendors of equipment for the size of current load required to supply the MFFF normal loads.

10 CFR 70.64 (a)(7) requires that the design of new facilities must provide for continued operation of essential utility services.

10 CFR 70.23(b) requires that the design bases of the principle structures, systems, and components, and the quality assurance program provide reasonable assurance of protection against natural phenomena and the consequences of accidents, and that the criteria in Appendix B of 10 CFR Part 50 will be used in determining the adequacy of the quality assurance program.

PS-E-15

LA Section 11.4.1.1.2, page 11.4-6

Resolve the apparent conflict in the statement on this page regarding the availability of emergency lighting. A statement is made that the 400 VDC battery of each train of uninterruptible power for emergency lighting is capable of powering the emergency egress lighting for a period of one hour. IEEE Standard 446, referenced in Section 11.4.5 of the License Application, (and NFPA-101, paragraph 7.9.2.1) requires a

minimum capability of battery-backed emergency lighting systems of 1.5 hours, and Table 3.2.2 of this standard recommends a 2 hour design requirement for some applications. Also, state whether there is a need for certain process operations to continue to be performed beyond the capacity requirement of the emergency lighting system, and if so, describe the standby lighting provisions that have been made which allow for personnel to continue these activities.

10 CFR 70.64 (a)(4) requires that the design of new facilities must provide for adequate protection from environmental conditions and dynamic effects associated with normal operations, maintenance, testing, and postulated accidents that could lead to loss of safety functions.

PS-E-16

LA Section 15.3

Explain what facilities within the MFFF will be used for calibration and maintenance of active engineered electrical components used as IROFS, including storage of test equipment, control of calibration standards, collection and storage of performance data used in the development of calibration procedures, and repair of active engineered IROFS that fail in service. Provide a label on the General Arrangement drawings for the room within the MOX FFF where the electrical equipment calibration and maintenance shop activities will take place.

10 CFR 70.64 (a)(8) requires that the design of items relied on for safety must provide for adequate inspection, testing, and maintenance, to ensure their availability and reliability to perform their function when needed. NUREG 1718 Section 15.3.4.3.A states that a license application is acceptable if it adequately addresses “an assessment of whether components and support systems need to be individually maintained to ensure the availability and reliability of specific safety controls.”

NUREG 1718 Section 15.3.4.3.B.i states that a license application is acceptable if it adequately addresses “the surveillance monitoring function, its responsible organization, and the conduct of surveillance/monitoring at specified frequencies to measure the degree to which safety functions or safety controls meet performance specifications. This activity is used in setting preventive maintenance frequencies for safety controls and the determination of performance trends for safety controls. How results from incident investigations...and identified root causes are used to modify the affected maintenance function and eliminate or minimize the root cause from recurring should be addressed. For surveillance tests that can be done only while equipment is out of service, proper compensatory measures should be prescribed.”

NUREG 1718 Section 15.3.4.3.B.iii states that a license application is acceptable if it adequately addresses “a description of the preventative maintenance function that contains a commitment to conduct preplanned and scheduled periodic refurbishing or partial or complete overhaul for the purpose of providing reasonable assurance that the reliability and availability goals for the IROFS will continue to be met even with unplanned outages. This activity includes the results of the surveillance/monitoring component of maintenance. Instrument calibration and testing should be addressed as part of this component.”

PS-E-17

LA Section 15.3

Identify what methodology will be used to establish the initial set of calibration and surveillance intervals needed to adequately maintain active engineered electrical IROFS so that they are available and reliable when needed. Describe the methodology that will be used to identify any required changes to the initial calibration surveillance intervals and how this information will be incorporated into the implementation of the surveillance program.

10 CFR 70.64 (a)(8) requires that the design of items relied on for safety must provide for adequate inspection, testing, and maintenance, to ensure their availability and reliability to perform their function when needed. NUREG 1718 Section 15.3.4.3.B.i states that a license application is acceptable if it adequately addresses “the surveillance monitoring function, its responsible organization, and the conduct of surveillance/monitoring at specified frequencies to measure the degree to which safety functions or safety controls meet performance specifications. This activity is used in setting preventive maintenance frequencies for safety controls and the determination of performance trends for safety controls. How results from incident investigations...and identified root causes are used to modify the affected maintenance function and eliminate or minimize the root cause from recurring should be addressed. For surveillance tests that can be done only while equipment is out of service, proper compensatory measures should be prescribed.”

NUREG 1718 Section 15.3.4.3.B.iii states that a license application is acceptable if it adequately addresses “a description of the preventative maintenance function that contains a commitment to conduct preplanned and scheduled periodic refurbishing or partial or complete overhaul for the purpose of providing reasonable assurance that the reliability and availability goals for the IROFS will continue to be met even with unplanned outages. This activity includes the results of the surveillance/monitoring component of maintenance. Instrument calibration and testing should be addressed as part of this component.”

PS-E-18

License Application Sections 11.4.3

Provide a brief description of the analysis performed to assure that power will continually be supplied to critical IROFS in the event of a fire occurring in either the electrical equipment rooms or battery rooms housing equipment for either train of the emergency power system or in the control room or alternate control room. Include a discussion of how an operator will be able to verify that the IROFS (e.g., VHD fans) are still functioning to perform their required safety actions, as well as a discussion regarding how no single failure of an emergency power train component can result in a fire which has the potential for rendering the other train inoperable or prevents a facility operator from assessing the status of critical IROFS.

10 CFR 70.61 paragraphs (b) and (c) require that engineered controls, administrative controls, or both shall be applied to reduce the likelihood of occurrence or the severity of consequence of high consequence and intermediate-consequence events.

10 CFR 70.61 (e) requires each engineered or administrative control or control system necessary to comply with paragraphs (b), (c), or (d) of Section 70.61 shall be designated as an item relied on for safety, and that the safety program shall ensure that each item relied on for safety will be available and reliable to perform its intended function when needed and in the context of the performance requirements of section 70.61.

10 CFR 70.64 (a)(4) requires that the design of new facilities must provide for adequate protection from environmental conditions and dynamic effects associated with normal operations, maintenance, testing, and postulated accidents that could lead to loss of safety functions.

10 CFR 70.64 (a)(7) requires that the design of new facilities must provide for continued operation of essential utility services.

10 CFR 70.64 (b) requires that system design and facility layout must be based on defense-in-depth practices, and that to the extent practicable, the design must incorporate a preference for the selection of engineered controls over administrative controls to increase the overall system reliability, and features that enhance safety by reducing challenges to items relied on for safety.

NUREG 1718 Section 5.4.3.1.D states that the applicant's methodology for applying likelihoods to the accidents examined...should "address any design bases that ensure that the principal SSC will function as intended (e.g., safety margins for criticality)."

NUREG 1718 Section 5.4.3.1.E states that the applicant's safety assessment of the design bases includes a process hazard analysis and accident sequence identification ... in which the applicant "Indicates the controlled parameters for safe operation, provides the limiting values of any controlled parameter, and explains and assesses the means of controlling those parameters to within those limiting values," as well as "explains for processes vulnerable to criticality accidents, why it is expected that the given design and design bases will meet the double contingency requirement of 10 CFR 70.64(a)(9)."

NUREG 1718 Section 5.4.3.2.B.iii states that an acceptable ISA meets the following criteria for a description of facility processes:

- (c) Process design and equipment, including a discussion of the process design, equipment, and instrumentation that is sufficiently detailed to permit an adequate understanding of the results of the ISA."

NUREG 1718 Section 11.4.2 states: Typically, specific design considerations for electrical systems include two physically independent offsite power sources with redundant and independent onsite ac and dc power sources that should be designed with the following:

- B. Electrical and physical separation to ensure that any required independence is maintained;
- C. No single failure vulnerability;

F. Status monitoring of the behavior of the systems and components that are identified as IROFS;

PS-E-19

License Application Section 11.8.1.7

Clarify the description of the emergency diesel generator fuel oil storage tank vault. Currently the description states that the vault is heated during cold weather conditions so that fuel in the tank does not undergo gelling. Section 11.8.1.7.4 also indicates that the normal power supply system provides power to the emergency generator major components, instrumentation, and valves. In the event of a loss of normal power which can occur for an extended period during cold weather conditions, what provisions have been provided to maintain the availability and reliability of the emergency diesel generator fuel oil system?

10 CFR 70.64 (a)(7) requires that the design of new facilities must provide for continued operation of essential utility services.

10 CFR 70.61 paragraphs (b) and (c) require that engineered controls, administrative controls, or both shall be applied to reduce the likelihood of occurrence or the severity of consequence of high consequence and intermediate-consequence events.

10 CFR 70.61 (e) requires each engineered or administrative control or control system necessary to comply with paragraphs (b), (c), or (d) of Section 70.61 shall be designated as an item relied on for safety, and that the safety program shall ensure that each item relied on for safety will be available and reliable to perform its intended function when needed and in the context of the performance requirements of section 70.61.

10 CFR 70.64 (a)(4) requires that the design of new facilities must provide for adequate protection from environmental conditions and dynamic effects associated with normal operations, maintenance, testing, and postulated accidents that could lead to loss of safety functions.

10 CFR 70.64 (b) requires that system design and facility layout must be based on defense-in-depth practices, and that to the extent practicable, the design must incorporate a preference for the selection of engineered controls over administrative controls to increase the overall system reliability, and features that enhance safety by reducing challenges to items relied on for safety.

NUREG 1718 Section 5.4.3.2.B.xi states: "The applicant describes the essential features of each IROFS that are required to achieve adequate reliability. The applicant should provide sufficient information about engineered hardware controls to permit an evaluation that, in principle, [demonstrates that] controls of this type will have adequate reliability.

PS-E-20

License Application Section 11.4.2.2

Clarify the description of the standby diesel generator starting and loading sequence and the “auxiliary PLC” that controls this operation. The description identifies that either one or two prioritized load groups will be applied by the “auxiliary PLC” depending on the availability of each standby diesel generator. Provide a clarification as to whether the “auxiliary PLC is the same as the “Utility Auxiliary Control System” described in Section 11.5.1.2 or whether this is a dedicated PLC acting as the Standby Diesel Generator load sequencer system. Provide a description of the methodology used to identify which loads among each prioritized group should be added in sequence, or whether the standby diesel generators are capable of accepting its assigned complete load of the MFFF priority group simultaneously. Verify that the PLC does not have a mode of operation which can override a required functional operational requirement while in test mode, nor will not potentially mask an unavailable operating function while in test mode.

This question is needed for regulatory clarification of the functions provided by the design of the standby power system.

**Mixed Oxide Fuel Fabrication Facility—Licensing Review
Request for Additional Information
Plant Systems –Instrumentation and Control Design**

PS-I&C-1

ISA Section 5.3 and LA Sections 11.5.1.1.3 and 11.5.1.3

Setpoint Methodology

Provide a description of the methodology that will be used to establish allowances in the settings and calibrated ranges of instruments and devices used as IROFS due to uncertainties in instrumentation channel accuracies and instrument drift that can occur between successive calibration surveillances. In this description, address how the effects of uncertainties (e.g., calibration standards, calibration equipment, calibration methods, instrument reference accuracy, power supply fluctuations, normal and anticipated abnormal ambient environmental effects, radiation exposure, analog-to-digital conversion, digital signal processing, instrument performance during design basis events, process dependencies and dynamics, and installation-based effects, etc.) will be accounted for in the settings of instruments used as IROFS. Identify how a safety margin will be established to accommodate these instrument channel uncertainties that is different from any margin which is allocated to account for process modeling error or process dynamics uncertainties. Describe how the implementation of this methodology will assure that all IROFS will perform their intended safety functions before the process analytical limit is reached, so as to meet the performance requirements of 10 CFR 70.61.

10 CFR 70.64 (a)(10) requires that the design of new facilities provide for the inclusion of instrumentation and control systems to monitor and control the behavior of items relied on for safety.

10 CFR 70.61 (e) requires each engineered or administrative control or control system necessary to comply with paragraphs (b), (c), or (d) of Section 70.61 shall be designated as an item relied on for safety, and that the safety program shall ensure that each item relied on for safety will be available and reliable to perform its intended function when needed and in the context of the performance requirements of section 70.61.

10 CFR 70.64 (a)(4) requires that the design of new facilities must provide for adequate protection from environmental conditions and dynamic effects associated with normal operations, maintenance, testing, and postulated accidents that could lead to loss of safety functions.

10 CFR 70.62 (c)(vi) requires that each applicant conduct and maintain an integrated safety analysis that identifies each item relied on for safety, the characteristics of its preventative, mitigative, or other safety function, and the assumptions and conditions under which the item is relied upon to support compliance with the performance requirements of Section 70.61.

Enclosure 2

10 CFR 70.62 (d) requires that management measures shall be established to ensure compliance with the performance requirements of Section 70.61. The management measures shall ensure that engineered and administrative controls and control systems that are identified as items relied on for safety are designed, implemented, and maintained, as necessary, to ensure that they are available and reliable to perform their function when needed, to comply with the performance requirements of Section 70.61.

NUREG 1718 Section 5.3.2 states that the ISA Summary should contain a description of “IROFS for all accidents in each process sufficiently to understand their safety function in meeting the appropriate consequence and likelihood requirements of 10 CFR 70.61,” as well as the “information... demonstrating compliance with baseline design criteria required by 10 CFR 70.64(a)(1) through (5) and (7) through (10) for new facilities...and required to be submitted in accordance with 10 CFR 70.65 (b)(4). Since these elements all bear on the adequacy of IROFS, it is efficient to include their review in the ISA Summary review.”

NUREG 1718 Section 5.4.3.1.D states that the applicant’s methodology for applying likelihoods to the accidents examined...should “address any design bases that ensure that the principal SSC will function as intended (e.g., safety margins for criticality).”

NUREG 1718 Section 5.4.3.1.F states that the description of principal SSCs in the ISA summary should include: “For each principal SSC, the parameters that will be specified or controlled for safety and the ranges and values of those parameters that constitutes the design bases. For active engineered controls, the applicant states the type of sensing and the type of control device....The applicant demonstrates that these parameters are consistent with the process description ...and incorporates sufficient safety margins to account for uncertainties.”

NUREG 1718 Section 5.4.3.2.B.xi states: “The applicant describes the essential features of each IROFS that are required to achieve adequate reliability. The applicant should provide sufficient information about engineered hardware controls to permit an evaluation that, in principle, [demonstrates that] controls of this type will have adequate reliability. Because the likelihood of failure of IROFS often depends on safety margins, the applicant should, in general, describe the safety parameter controlled by the item, the safety limit on the parameter, and the margin to true failure. For IROFS that are administrative controls, the applicant should sufficiently describe the nature of the action or prohibition involved to permit an understanding that, in principle, [demonstrates that] adherence to it should be reliable.

Finally, NUREG 1718 Section 11.4.3 states...” The instrument channels and associated logic should be designed with the following:

- D. Adequate instrument spans, setpoints, and control ranges to ensure proper monitoring and control of IROFS”

PS-I&C-2

ISA Sections 5.2.2.4 and 5.3 and LA Sections 11.5.1.1.3 and 11.5.1.3

Equipment Qualification

Identify whether there are any active engineered process instruments, PLCs, or devices used as IROFS which must function to mitigate an identified process hazard event following chronic or acute exposure to or during exposure to potential identified chemical hazards. Provide a description of how such IROFS will be assured of being reliable and available to perform their required safety functions in the event of such chemical exposure. Clarify the statement in Section 11.5.1.3 that "IEEE-323 is used as a basis for the program of environmental qualification for normal, abnormal, and accident conditions," as it applies to the identification of the qualification parameters and qualification testing needed to assure the reliability of instrumentation and control IROFS which may be exposed to continual or occasional chemical atmospheres or potential chemical hazards.

10 CFR 70.61 (e) requires each engineered or administrative control or control system necessary to comply with paragraphs (b), (c), or (d) of Section 70.61 shall be designated as an item relied on for safety, and that the safety program shall ensure that each item relied on for safety will be available and reliable to perform its intended function when needed and in the context of the performance requirements of section 70.61.

10 CFR 70.64 (a)(4) requires that the design of new facilities must provide for adequate protection from environmental conditions and dynamic effects associated with normal operations, maintenance, testing, and postulated accidents that could lead to loss of safety functions.

10 CFR 70.62 (d) requires that management measures shall be established to ensure compliance with the performance requirements of Section 70.61. The management measures shall ensure that engineered and administrative controls and control systems that are identified as items relied on for safety are designed, implemented, and maintained, as necessary, to ensure that they are available and reliable to perform their function when needed, to comply with the performance requirements of Section 70.61.

NUREG 1718 Section 5.4.3.1.D states that the applicant's methodology for applying likelihoods to the accidents examined...should "address any design bases that ensure that the principal SSC will function as intended (e.g., safety margins for criticality)."

NUREG 1718 Section 5.4.3.1.F states that the description of principal SSCs in the ISA summary should include: "For each principal SSC, the parameters that will be specified or controlled for safety and the ranges and values of those parameters that constitutes the design bases. For active engineered controls, the applicant states the type of sensing and the type of control device....The applicant demonstrates that these parameters are consistent with the process description ...and incorporates sufficient safety margins to account for uncertainties."

PS-I&C-3

ISA Section 4.5.1.2.1 and License Application Sections 11.5.1.2.1 and 11.5.1.3

Interface between Utility Control System and Emergency Control System

Clarify the description in Section 11.5.1.2.1 of the License Application regarding the design of the Utility Normal Control System. The statement indicates that the Utility Normal Control System communicates “data” to the Emergency Control System, while the description of the Emergency Control System states that it is “constructed from traditional electromechanical relays, solid state electronic systems, display devices, and manually operated switches,” and that “Software programmable devices (such as PLCs PCs and computers), are not utilized to satisfy a safety or emergency function.” If necessary, provide additional description in Section 11.5.1.3 of the License Application to identify how the Emergency Control System utilizes the data transmitted to it from the Utility Control System, and whether this data is relied upon for the accomplishment of safety related functions.

10 CFR 70.61 paragraphs (b) and (c) require that engineered controls, administrative controls, or both shall be applied to reduce the likelihood of occurrence or the severity of consequence of high consequence and intermediate-consequence events.

NUREG 1718 Section 5.3.2 states that the ISA Summary should contain a description of “IROFS for all accidents in each process sufficiently to understand their safety function in meeting the appropriate consequence and likelihood requirements of 10 CFR 70.61,” as well as the “information... demonstrating compliance with baseline design criteria required by 10 CFR 70.64(a)(1) through (5) and (7) through (10) for new facilities...and required to be submitted in accordance with 10 CFR 70.65 (b)(4). Since these elements all bear on the adequacy of IROFS, it is efficient to include their review in the ISA Summary review.”

NUREG 1718 Section 5.4.3.2.B.iii states that an acceptable ISA meets the following criteria for a description of facility processes:

- “(c) Process design and equipment, including a discussion of the process design, equipment, and instrumentation that is sufficiently detailed to permit an adequate understanding of the results of the ISA.”
- (d) Process operating ranges and limits, including the operating ranges and limits for measured process variables (e.g., temperatures, pressures, flows, and compositions) that are controlled by the IROFS to ensure safe operation of the process.”

PS-I&C-4

ISA Summary Section 4.5.1.2.1 and License Application Sections 11.5.1.2.1 & 11.5.1.3

Interface between Utility Control System and Emergency Control System

Clarify the description in Section 11.5.1.3 of the License Application regarding the design of the Emergency Control System. The statement indicates that the Utility Normal

Control System communicates “data” to the Emergency Control System, while the description of the Emergency Control System states that it is “constructed from traditional electromechanical relays, solid state electronic systems, display devices, and manually operated switches,” and that “Software programmable devices (such as PLCs PCs and computers), are not utilized to satisfy a safety or emergency function.” Provide a description of any interface between the Emergency Control System and components within the actuator motor control center that cause the actuated components to open/close or start/stop, and either verify that these components are not required to accomplish safety actions, or do not require the use of software programmable instructions or, if they do, provide a description of how these components are qualified to perform their required safety actions.

NUREG 1718 Section 5.3.2 states that the ISA Summary should contain a description of “IROFS for all accidents in each process sufficiently to understand their safety function in meeting the appropriate consequence and likelihood requirements of 10 CFR 70.61,” as well as the “information... demonstrating compliance with baseline design criteria required by 10 CFR 70.64(a)(1) through (5) and (7) through (10) for new facilities...and required to be submitted in accordance with 10 CFR 70.65 (b)(4). Since these elements all bear on the adequacy of IROFS, it is efficient to include their review in the ISA Summary review.”

NUREG 1718 Section 5.4.3.2.B.iii states that an acceptable ISA meets the following criteria for a description of facility processes:

- “(c) Process design and equipment, including a discussion of the process design, equipment, and instrumentation that is sufficiently detailed to permit an adequate understanding of the results of the ISA.”
- (e) Process operating ranges and limits, including the operating ranges and limits for measured process variables (e.g., temperatures, pressures, flows, and compositions) that are controlled by the IROFS to ensure safe operation of the process.”

PS-I&C-5

ISA Section 4.5.1.2.2 and License Application Section 11.5.1.2

Utility Auxiliary Control System Design Basis

Clarify the description of the function served by the utility auxiliary controllers and workstations. Identify the functions served by and the conditions under which the utility auxiliary controllers workstations are expected to “provide alternate monitoring and control capability in the event that the normal utility control systems become compromised, disabled, or otherwise unavailable.” Specify the design basis conditions or events for which it is deemed necessary for the utility auxiliary workstations to be independent from, but located in the same normal utility control room D-301, albeit in a separate location from the normal utility control room workstations. Include in this discussion an evaluation of how such a system does not share a potential common mode failure mechanism with the normal utility control system. Alternatively, provide a discussion regarding why the likelihood for such potential common mode failure is considered to be negligible.

NUREG 1718 Section 5.3.2 states that the ISA Summary should contain a description of “IROFS for all accidents in each process sufficiently to understand their safety function in meeting the appropriate consequence and likelihood requirements of 10 CFR 70.61,” as well as the “information... demonstrating compliance with baseline design criteria required by 10 CFR 70.64(a)(1) through (5) and (7) through (10) for new facilities...and required to be submitted in accordance with 10 CFR 70.65 (b)(4). Since these elements all bear on the adequacy of IROFS, it is efficient to include their review in the ISA Summary review.”

NUREG 1718 Section 5.4.3.2.B.iii states that an acceptable ISA meets the following criteria for a description of facility processes:

- “(c) Process design and equipment, including a discussion of the process design, equipment, and instrumentation that is sufficiently detailed to permit an adequate understanding of the results of the ISA.”
- “(f) Process operating ranges and limits, including the operating ranges and limits for measured process variables (e.g., temperatures, pressures, flows, and compositions) that are controlled by the IROFS to ensure safe operation of the process.”

PS-I&C-6

ISA Section 4.5.1.2.2 and License Application Section 11.5.1.2

Utility Auxiliary Control System Design Basis

Clarify the purpose of the Utility Auxiliary Control System and the statement that the “Utility Auxiliary Control System controllers are not IROFS.” The License Application states that the “function of the Utility Auxiliary Control System is to ensure that the Electrical Power Distribution and HVAC utility systems shall continue to operate as needed to prevent or mitigate the consequences of an incident which may result in the release of radioactive material above acceptable limits, as defined in 10 CFR 70 beyond the confines of the facility.” Further, the Application states that “these controllers are provided where there is a possibility that the improper operation of the facility may create conditions that may result in the loss of the ability to prevent the release of radioactive material.” Describe the potential events which have been considered that make it reasonably necessary to provide a Utility Auxiliary Control System and provide a clarifying basis for the statement that the active engineered devices within this system which serve to ensure that the Electrical Power Distribution and HVAC utility systems continue to operate as needed are not identified as IROFS. Alternatively, provide a description of how the controls for the Electrical Power Distribution and HVAC utility systems required to perform safety actions are provided with a defense-in-depth design architecture in addition to the Emergency Control System which is equipped with components that are designated as IROFS.

10 CFR 70.61 paragraphs (b) and (c) require that engineered controls, administrative controls, or both shall be applied to reduce the likelihood of occurrence or the severity of consequence of high consequence and intermediate-consequence events.

10 CFR 70.61 (e) requires each engineered or administrative control or control system necessary to comply with paragraphs (b), (c), or (d) of Section 70.61 shall be designated

as an item relied on for safety, and that the safety program shall ensure that each item relied on for safety will be available and reliable to perform its intended function when needed and in the context of the performance requirements of section 70.61.

10 CFR 70.64 (a)(7) requires that the design of new facilities must provide for continued operation of essential utility services.

10 CFR 70.64 (b) requires that system design and facility layout must be based on defense-in-depth practices, and that to the extent practicable, the design must incorporate a preference for the selection of engineered controls over administrative controls to increase the overall system reliability, and features that enhance safety by reducing challenges to items relied on for safety.

PS-I&C-7

ISA Summary Section 4.5.1.1.3 and License Application Section 11.5.1.1.3

Safety Control System Operation and Interface with Normal Control System and Facility Operators

Clarify the description of the intended operations and required interfaces among the safety controller, the normal controller, and the required actions to be taken by the facility operators to provide for a better understanding of this operation. In Section 1.5.1.1.3, the statement is made that the “safety controller action remains effective, blocking any automatic continuation of the process until the safety controller is released, with operator key switches, after restoring the operating condition back to a safe condition.” Provide a step-by-step description of how the safety controller communicates with the normal controller and the facility operator to signal that a safety action has taken place, what happens within the normal controller when such a signal is received, how an operator is informed that the normal controller automatic operation has been “frozen”, what steps the operator must take to manually operate the normal controller with the process in the potentially unsafe condition while the safety controller maintains its blocking action, what provisions have been made within the normal controller to prevent its continued automatic operation from suddenly resuming while the unsafe condition is being cleared, how the process may be manipulated with the normal controller only in manual mode to “back-out” of the incorrect action without accidental operation of the actuated component being blocked by the safety action, what information is received by the operator to determine and confirm that a safe process condition has been reached, and what actions are required to take place within both the normal and the safety controllers when the operator manipulates the “operator key switches” to remove the blocking signals. For the few cases where the same shared sensor is providing a signal to both the normal and safety controllers, provide a description of the provisions that have been made to confirm to the safety controller and the facility operator that the unsafe condition is no longer present, and that it is permissible to reset the safety controller and resume operations with the normal controller. Also provide a description of the provision that has been made to prevent the normal controller from automatically resuming automatic control upon reset of the blocking signals from the safety controller without some form of positive action by the facility operators to do so.

10 CFR 70.64 (a)(10) requires that the design of new facilities provide for the inclusion of instrumentation and control systems to monitor and control the behavior of items relied on for safety.

10 CFR 70.61 paragraphs (b) and (c) require that engineered controls, administrative controls, or both shall be applied to reduce the likelihood of occurrence or the severity of consequence of high consequence and intermediate-consequence events.

10 CFR 70.61 (e) requires each engineered or administrative control or control system necessary to comply with paragraphs (b), (c), or (d) of Section 70.61 shall be designated as an item relied on for safety, and that the safety program shall ensure that each item relied on for safety will be available and reliable to perform its intended function when needed and in the context of the performance requirements of section 70.61.

10 CFR 70.62 (c)(vi)) requires that each applicant conduct and maintain an integrated safety analysis that identifies each item relied on for safety, the characteristics of its preventative, mitigative, or other safety function, and the assumptions and conditions under which the item is relied upon to support compliance with the performance requirements of Section 70.61.

NUREG 1718 Section 5.3.2 states that the ISA Summary should contain a description of "IROFS for all accidents in each process sufficiently to understand their safety function in meeting the appropriate consequence and likelihood requirements of 10 CFR 70.61," as well as the "information... demonstrating compliance with baseline design criteria required by 10 CFR 70.64(a)(1) through (5) and (7) through (10) for new facilities...and required to be submitted in accordance with 10 CFR 70.65 (b)(4). Since these elements all bear on the adequacy of IROFS, it is efficient to include their review in the ISA Summary review."

NUREG 1718 Section 5.4.3.2.B.xi states: "The applicant describes the essential features of each IROFS that are required to achieve adequate reliability. The applicant should provide sufficient information about engineered hardware controls to permit an evaluation that, in principle, [demonstrates that] controls of this type will have adequate reliability. Because the likelihood of failure of IROFS often depends on safety margins, the applicant should, in general, describe the safety parameter controlled by the item, the safety limit on the parameter, and the margin to true failure. For IROFS that are administrative controls, the applicant should sufficiently describe the nature of the action or prohibition involved to permit an understanding that, in principle, [demonstrates that] adherence to it should be reliable. The applicant should indicate features of the IROFS that affect its independence from other IROFS, such as reliance on the same power supplies."

PS-I&C-8

License Application Sections 11.5.1.1 through 11.5.1.3

Effects of Loss of Normal Power Supply to the Utility Control System, the Safety Control System and the Emergency Control System

Describe the effects of a loss of normal power supply to the components of the Utility Control System, the Safety Control System, and the Emergency Control System identified as IROFS, including the effects of this condition on operator interface devices, such as workstations and hardwired control panels. Provide a description that is sufficiently complete to allow one to understand the potential duration that these systems may be inoperable, the bases for inclusion of vital and emergency power supplies, the anticipated performance of the controllers within these systems when subject to a momentary loss of power, the behavior of these systems when power is restored, and the potential consequences to actuated components, such as isolation valves and critical HVAC fans, when the power to the controllers for these devices is interrupted and subsequently restored. Describe the consequences of any potential interactions, if any, among these systems during potential events where power may be momentarily lost to active engineered components, and then is suddenly restored. For example, describe the expected interaction that will take place between a workstation and its associated controller when power is momentarily lost to the workstation, but not to the controller.

10 CFR 70.64 (a)(10) requires that the design of new facilities provide for the inclusion of instrumentation and control systems to monitor and control the behavior of items relied on for safety.

10 CFR 70.61 (e) requires each engineered or administrative control or control system necessary to comply with paragraphs (b), (c), or (d) of Section 70.61 shall be designated as an item relied on for safety, and that the safety program shall ensure that each item relied on for safety will be available and reliable to perform its intended function when needed and in the context of the performance requirements of section 70.61.

10 CFR 70.64 (a)(7) requires that the design of new facilities must provide for continued operation of essential utility services.

10 CFR 70.62 (d) requires that management measures shall be established to ensure compliance with the performance requirements of Section 70.61. The management measures shall ensure that engineered and administrative controls and control systems that are identified as items relied on for safety are designed, implemented, and maintained, as necessary, to ensure that they are available and reliable to perform their function when needed, to comply with the performance requirements of Section 70.61.

NUREG 1718 Section 5.4.3.1.D states that the applicant's methodology for applying likelihoods to the accidents examined...should "address any design bases that ensure that the principal SSC will function as intended (e.g., safety margins for criticality)."

NUREG 1718 Section 5.4.3.1.E states that the applicant's safety assessment of the design bases includes a process hazard analysis and accident sequence identification ... in which the applicant "Indicates the controlled parameters for safe operation, provides the limiting values of any controlled parameter, and explains and assesses the means of controlling those parameters to within those limiting values," as well as "explains for processes vulnerable to criticality accidents, why it is expected that the given design and design bases will meet the double contingency requirement of 10 CFR 70.64(a)(9)."

PS-I&C-9

ISA Summary Sections 4.5.1.1.3 and 5.3 and License Application Section 11.5.1.1.3

Response Time Characteristics of the Safety Control System and Emergency Control System

Based on the results of process hazards analyses and the intended performance requirements of IROFS designed to mitigate those hazards, identify the fastest required response time for any of the required IROFS actions served by the sensing channels implemented by the Safety Control System (including PLC response) or the Emergency Control System (e.g., glovebox differential pressure switches) that is adequate to achieve reliability. Provide a discussion that demonstrates that the instrument channels associated with the Safety Control System or the Emergency Control System are designed to meet this response time requirement. Include an analysis of the response capabilities for analog input changes-to-discrete output response required from the control systems as well as discrete input changes-to-discrete output responses from the control system.

10 CFR 70.64 (a)(10) requires that the design of new facilities provide for the inclusion of instrumentation and control systems to monitor and control the behavior of items relied on for safety.

10 CFR 70.61 paragraphs (b) and (c) require that engineered controls, administrative controls, or both shall be applied to reduce the likelihood of occurrence or the severity of consequence of high consequence and intermediate-consequence events.

10 CFR 70.61 (e) requires each engineered or administrative control or control system necessary to comply with paragraphs (b), (c), or (d) of Section 70.61 shall be designated as an item relied on for safety, and that the safety program shall ensure that each item relied on for safety will be available and reliable to perform its intended function when needed and in the context of the performance requirements of section 70.61.

10 CFR 70.64 (a)(4) requires that the design of new facilities must provide for adequate protection from environmental conditions and dynamic effects associated with normal operations, maintenance, testing, and postulated accidents that could lead to loss of safety functions.

10 CFR 70.64 (a)(7) requires that the design of new facilities must provide for continued operation of essential utility services.

10 CFR 70.64 (b) requires that system design and facility layout must be based on defense-in-depth practices, and that to the extent practicable, the design must incorporate a preference for the selection of engineered controls over administrative controls to increase the overall system reliability, and features that enhance safety by reducing challenges to items relied on for safety.

10 CFR 70.62 (c)(vi) requires that each applicant conduct and maintain an integrated safety analysis that identifies each item relied on for safety, the characteristics of its preventative, mitigative, or other safety function, and the assumptions and conditions

under which the item is relied upon to support compliance with the performance requirements of Section 70.61.

10 CFR 70.62 (d) requires that management measures shall be established to ensure compliance with the performance requirements of Section 70.61. The management measures shall ensure that engineered and administrative controls and control systems that are identified as items relied on for safety are designed, implemented, and maintained, as necessary, to ensure that they are available and reliable to perform their function when needed, to comply with the performance requirements of Section 70.61.

PS-I&C-10

License Application Section 11.5.1.1.3

Safety System Software Quality

Provide a description of the processes used to assure that the quality of the software used in IROFS (such as Safety PLCs) to accomplish safety functions will ensure that these IROFS will be available and reliable when needed to accomplish their required safety functions. Include a discussion of the processes used to assure the quality of the applications software prepared specifically to accomplish the MFFF safety functions and software that has been developed to control the operation of the IROFS by the applicable equipment vendors. In the event that any software validation and verification processes is being or has been performed by organizations other than the MFFF project team, identify the process used by the MFFF project team to review and accept the results of such validation and verification activities.

10 CFR 70.61 (e) requires each engineered or administrative control or control system necessary to comply with paragraphs (b), (c), or (d) of Section 70.61 shall be designated as an item relied on for safety, and that the safety program shall ensure that each item relied on for safety will be available and reliable to perform its intended function when needed and in the context of the performance requirements of section 70.61.

10 CFR 70.62 (d) requires that management measures shall be established to ensure compliance with the performance requirements of Section 70.61. The management measures shall ensure that engineered and administrative controls and control systems that are identified as items relied on for safety are designed, implemented, and maintained, as necessary, to ensure that they are available and reliable to perform their function when needed, to comply with the performance requirements of Section 70.61.

10 CFR 70.65 (b)(4) requires that the integrated safety analysis summary must contain information that demonstrates the licensee's compliance with the performance requirements of Section 70.61, including a description of the management measures; the requirements for criticality monitoring and alarms in Section 70.24; and if applicable, the requirements of Section 70.64.

NUREG 1718 Section 5.4.3.2.B.xi states: "The applicant describes the essential features of each IROFS that are required to achieve adequate reliability. The applicant should provide sufficient information about engineered hardware controls to permit an evaluation that, in principle, [demonstrates that] controls of this type will have adequate

reliability. Because the likelihood of failure of IROFS often depends on safety margins, the applicant should, in general, describe the safety parameter controlled by the item, the safety limit on the parameter, and the margin to true failure. For IROFS that are administrative controls, the applicant should sufficiently describe the nature of the action or prohibition involved to permit an understanding that, in principle, [demonstrates that] adherence to it should be reliable. The applicant should indicate features of the IROFS that affect its independence from other IROFS, such as reliance on the same power supplies.”

PS-I&C-11

ISA Summary Sections 4.5 and 5.3, and License Application Sections 11.5.1.1.3 and 11.5.1.3

Diversity and Defense-in-Depth Analysis

Provide a description of the analysis that was performed to ascertain that two redundant trains of safety channels made up with identical (or nearly identical) equipment within each train provides sufficient diversity and defense-in-depth to assure that the system of IROFS designed to prevent or mitigate the effects of identified process hazards will be sufficiently available and reliable to perform their required safety action when needed.

10 CFR 70.64 (a)(10) requires that the design of new facilities provide for the inclusion of instrumentation and control systems to monitor and control the behavior of items relied on for safety.

10 CFR 70.61 paragraphs (b) and (c) require that engineered controls, administrative controls, or both shall be applied to reduce the likelihood of occurrence or the severity of consequence of high consequence and intermediate-consequence events.

10 CFR 70.61 (e) requires each engineered or administrative control or control system necessary to comply with paragraphs (b), (c), or (d) of Section 70.61 shall be designated as an item relied on for safety, and that the safety program shall ensure that each item relied on for safety will be available and reliable to perform its intended function when needed and in the context of the performance requirements of section 70.61.

10 CFR 70.64 (b) requires that system design and facility layout must be based on defense-in-depth practices, and that to the extent practicable, the design must incorporate a preference for the selection of engineered controls over administrative controls to increase the overall system reliability, and features that enhance safety by reducing challenges to items relied on for safety.

10 CFR 70.62 (d) requires that management measures shall be established to ensure compliance with the performance requirements of Section 70.61. The management measures shall ensure that engineered and administrative controls and control systems that are identified as items relied on for safety are designed, implemented, and maintained, as necessary, to ensure that they are available and reliable to perform their function when needed, to comply with the performance requirements of Section 70.61.

NUREG 1718 Section 11.4.3 states: “Typically, specific design considerations for I&C systems include redundant and/or diverse instrument channels with coincident logic providing automatic actuation with additional manual operation capability. The instrument channels and associated logic should be designed with the following:

- B. Electrical, physical, and control/protection separation to ensure that any required redundancy and independence are maintained”

PS-I&C-12

ISA Summary Sections 4.5.1.1.3 and 5.3 and License Application Section 11.5.1.1.3

Design Characteristics of the Safety Control System

Provide a discussion summarizing the analysis of the redundant safety control system trains utilizing identical safety PLCs in each train that addresses how the potential for common cause failure within the two control system trains was evaluated. Describe how the potential for common cause failure was addressed for hardware and software in the Safety PLCs as well as for other components performing redundant safety actions.

10 CFR 70.61 (e) requires each engineered or administrative control or control system necessary to comply with paragraphs (b), (c), or (d) of Section 70.61 shall be designated as an item relied on for safety, and that the safety program shall ensure that each item relied on for safety will be available and reliable to perform its intended function when needed and in the context of the performance requirements of section 70.61.

10 CFR 70.64 (b) requires that system design and facility layout must be based on defense-in-depth practices, and that to the extent practicable, the design must incorporate a preference for the selection of engineered controls over administrative controls to increase the overall system reliability, and features that enhance safety by reducing challenges to items relied on for safety.

10 CFR 70.62 (d) requires that management measures shall be established to ensure compliance with the performance requirements of Section 70.61. The management measures shall ensure that engineered and administrative controls and control systems that are identified as items relied on for safety are designed, implemented, and maintained, as necessary, to ensure that they are available and reliable to perform their function when needed, to comply with the performance requirements of Section 70.61.

NUREG 1718 Section 5.4.3.1.D states that the applicant’s methodology for applying likelihoods to the accidents examined...should “address any design bases that ensure that the principal SSC will function as intended (e.g., safety margins for criticality).”

NUREG 1718 Section 5.4.3.1.F states that the description of principal SSCs in the ISA summary should include: “For each principal SSC, the parameters that will be specified or controlled for safety and the ranges and values of those parameters that constitutes the design bases. For active engineered controls, the applicant states the type of sensing and the type of control device....The applicant demonstrates that these

parameters are consistent with the process description ...and incorporates sufficient safety margins to account for uncertainties.”

NUREG 1718 Section 5.4.3.2.B.v.d states “The method for evaluation of the likelihood of accident sequences...is considered acceptable if it provides reasonable assurance that the IROFS and management measures described comply with the graded performance criteria of 10 CFR 70.61” and that the criteria for acceptance includes:

- “(1) The method includes clearly showing how each IROFS involved acts to prevent or mitigate the accident sequence being evaluated.”
- “(2) When multiple IROFS are involved in an accident sequence, the method considers the interaction of all IROFS involved”...”that accounts for the impact of redundancy, independence, and surveillance to correct failures on the likelihood of occurrence of the accident.”

PS-I&C-13

ISA Summary Sections 4.5.1.1.3 and 5.3 and License Application Section 11.5.1.1.3

Application of Single Failure Criterion for Certain IROFS

Provide a general discussion on how the single failure criterion is being applied for the safety and the emergency control systems. Include a discussion of how the single failure criterion will be met for certain IROFS (e.g., counter scales within gloveboxes) for which it is not practical to have a redundant component providing a signal to the other safety train.

10 CFR 70.61 paragraphs (b) and (c) require that engineered controls, administrative controls, or both shall be applied to reduce the likelihood of occurrence or the severity of consequence of high consequence and intermediate-consequence events.

10 CFR 70.61 (e) requires each engineered or administrative control or control system necessary to comply with paragraphs (b), (c), or (d) of Section 70.61 shall be designated as an item relied on for safety, and that the safety program shall ensure that each item relied on for safety will be available and reliable to perform its intended function when needed and in the context of the performance requirements of section 70.61.

10 CFR 70.64 (a)(9) requires that the design must provide for criticality control including adherence to the double contingency principle.

10 CFR 70.65 (b)(8) requires that the integrated safety analysis summary must contain a descriptive list that identifies all items relied on for safety that are the sole item preventing or mitigating an accident sequence that exceeds the performance requirements of Section 70.61.

NUREG 1718 Section 5.4.3.1.F states that the description of principal SSCs in the ISA summary should include: “For each principal SSC, the parameters that will be specified or controlled for safety and the ranges and values of those parameters that constitutes the design bases. For active engineered controls, the applicant states the type of sensing and the type of control device....The applicant demonstrates that these

parameters are consistent with the process description ...and incorporates sufficient safety margins to account for uncertainties.”

NUREG 1718 Section 5.4.3.2.B.v.d states “The method for evaluation of the likelihood of accident sequences...is considered acceptable if it provides reasonable assurance that the IROFS and management measures described comply with the graded performance criteria of 10 CFR 70.61” and that the criteria for acceptance includes:

- “(1) The method includes clearly showing how each IROFS involved acts to prevent or mitigate the accident sequence being evaluated.”
- “(2) When multiple IROFS are involved in an accident sequence, the method considers the interaction of all IROFS involved”...”that accounts for the impact of redundancy, independence, and surveillance to correct failures on the likelihood of occurrence of the accident.”

NUREG 1718 Section 5.4.3.2.B.xi states: “The applicant describes the essential features of each IROFS that are required to achieve adequate reliability. The applicant should provide sufficient information about engineered hardware controls to permit an evaluation that, in principle, [demonstrates that] controls of this type will have adequate reliability. Because the likelihood of failure of IROFS often depends on safety margins, the applicant should, in general, describe the safety parameter controlled by the item, the safety limit on the parameter, and the margin to true failure. For IROFS that are administrative controls, the applicant should sufficiently describe the nature of the action or prohibition involved to permit an understanding that, in principle, [demonstrates that] adherence to it should be reliable. The applicant should indicate features of the IROFS that affect its independence from other IROFS, such as reliance on the same power supplies.”

NUREG 1718 Section 11.4.3 states: “Typically, specific design considerations for I&C systems include redundant and/or diverse instrument channels with coincident logic providing automatic actuation with additional manual operation capability. The instrument channels and associated logic should be designed with the following:

- C. No single failure vulnerability”

PS-I&C-14

License Application Sections 11.5.1.1.3 and 11.5.1.3

Adequacy of Separation and Isolation of Safety Functions from Non-safety Functions

Provide a description of the measures taken to assure the availability and reliability of IROFS by protecting them against potential faults in communications paths and power supplies with non-IROFS equipment. Describe how signal and power supply interfaces between the redundant trains of equipment performing safety functions and the non-IROFS equipment are protected such that no credible fault within a non-IROFS component will render both trains of safety equipment inoperable.

10 CFR 70.61 (e) requires each engineered or administrative control or control system necessary to comply with paragraphs (b), (c), or (d) of Section 70.61 shall be designated as an item relied on for safety, and that the safety program shall ensure that each item

relied on for safety will be available and reliable to perform its intended function when needed and in the context of the performance requirements of section 70.61.

10 CFR 70.64 (a)(4) requires that the design of new facilities must provide for adequate protection from environmental conditions and dynamic effects associated with normal operations, maintenance, testing, and postulated accidents that could lead to loss of safety functions.

10 CFR 70.64 (a)(7) requires that the design of new facilities must provide for continued operation of essential utility services.

10 CFR 70.64 (a)(9) requires that the design must provide for criticality control including adherence to the double contingency principle.

10 CFR 70.64 (b) requires that system design and facility layout must be based on defense-in-depth practices, and that to the extent practicable, the design must incorporate a preference for the selection of engineered controls over administrative controls to increase the overall system reliability, and features that enhance safety by reducing challenges to items relied on for safety.

10 CFR 70.62 (c)(vi)) requires that each applicant conduct and maintain an integrated safety analysis that identifies each item relied on for safety, the characteristics of its preventative, mitigative, or other safety function, and the assumptions and conditions under which the item is relied upon to support compliance with the performance requirements of Section 70.61.

10 CFR 70.62 (d) requires that management measures shall be established to ensure compliance with the performance requirements of Section 70.61. The management measures shall ensure that engineered and administrative controls and control systems that are identified as items relied on for safety are designed, implemented, and maintained, as necessary, to ensure that they are available and reliable to perform their function when needed, to comply with the performance requirements of Section 70.61.

NUREG 1718 Section 5.4.3.2.B.iii states that an acceptable ISA meets the following criteria for a description of facility processes:

- “(c) Process design and equipment, including a discussion of the process design, equipment, and instrumentation that is sufficiently detailed to permit an adequate understanding of the results of the ISA.”

NUREG 1718 Section 5.4.3.2.B.v.d states “The method for evaluation of the likelihood of accident sequences...is considered acceptable if it provides reasonable assurance that the IROFS and management measures described comply with the graded performance criteria of 10 CFR 70.61” and that the criteria for acceptance includes:

- “(1) The method includes clearly showing how each IROFS involved acts to prevent or mitigate the accident sequence being evaluated.”
- “(2) When multiple IROFS are involved in an accident sequence, the method considers the interaction of all IROFS involved”...“that accounts for the impact of redundancy, independence, and surveillance to correct failures on the likelihood of occurrence of the accident.”
- “(3) The method has objective criteria for evaluating, at least qualitatively, the likelihood of failure of individual IROFS. Such likelihood criteria should

include the following when applicable: means to limit potential failure modes, the magnitude of safety margins, the type of engineered equipment (active or passive) of human interaction that constitutes the IROFS, and the types and grading, if any, of the management measures applied to the IROFS.”

NUREG 1718 Section 5.4.3.2.B.xi states: “The applicant describes the essential features of each IROFS that are required to achieve adequate reliability. The applicant should provide sufficient information about engineered hardware controls to permit an evaluation that, in principle, [demonstrates that] controls of this type will have adequate reliability. Because the likelihood of failure of IROFS often depends on safety margins, the applicant should, in general, describe the safety parameter controlled by the item, the safety limit on the parameter, and the margin to true failure. For IROFS that are administrative controls, the applicant should sufficiently describe the nature of the action or prohibition involved to permit an understanding that, in principle, [demonstrates that] adherence to it should be reliable. The applicant should indicate features of the IROFS that affect its independence from other IROFS, such as reliance on the same power supplies.”

NUREG 1718 Section 11.4.3 states: “Typically, specific design considerations for I&C systems include redundant and/or diverse instrument channels with coincident logic providing automatic actuation with additional manual operation capability. The instrument channels and associated logic should be designed with the following:

C. No single failure vulnerability”

PS-I&C-15

LA Section 15.3

Instrument Calibration and Maintenance Facilities

Explain what facilities within the MFFF will be used for calibration and maintenance of active engineered instrumentation and controls components used as IROFS, including storage of test equipment, control of calibration standards, collection and storage of performance data used in the development of calibration procedures, and repair of active engineered IROFS that fail in service. Provide a label on the General Arrangement drawings for the room within the MOX FFF where the instrumentation and control calibration and maintenance activities will take place. Identify the area where calibration standards will be maintained within the environmental conditions needed to assure their accuracy sufficient to appropriately calibrate and maintain instrumentation and controls used as IROFS.

10 CFR 70.64 (a)(8) requires that the design of items relied on for safety must provide for adequate inspection, testing, and maintenance, to ensure their availability and reliability to perform their function when needed. NUREG 1718 Section 15.3.4.3.A states that a license application is acceptable if it adequately addresses “an assessment of whether components and support systems need to be individually maintained to ensure the availability and reliability of specific safety controls.”

NUREG 1718 Section 15.3.4.3.B.i states that a license application is acceptable if it adequately addresses “the surveillance monitoring function, its responsible organization, and the conduct of surveillance/monitoring at specified frequencies to measure the degree to which safety functions or safety controls meet performance specifications. This activity is used in setting preventive maintenance frequencies for safety controls and the determination of performance trends for safety controls. How results from incident investigations...and identified root causes are used to modify the affected maintenance function and eliminate or minimize the root cause from recurring should be addressed. For surveillance tests that can be done only while equipment is out of service, proper compensatory measures should be prescribed.”

NUREG 1718 Section 15.3.4.3.B.iii states that a license application is acceptable if it adequately addresses “a description of the preventative maintenance function that contains a commitment to conduct preplanned and scheduled periodic refurbishing or partial or complete overhaul for the purpose of providing reasonable assurance that the reliability and availability goals for the IROFS will continue to be met even with unplanned outages. This activity includes the results of the surveillance/monitoring component of maintenance. Instrument calibration and testing should be addressed as part of this component.”

PS-I&C-16

LA Section 15.3

Instrument Calibration and Maintenance Program

Identify what methodology will be used to establish the initial set of calibration and surveillance intervals needed to adequately maintain active engineered instrumentation and controls IROFS so that they are available and reliable when needed. Describe the methodology that will be used to identify any required changes to the initial calibration surveillance intervals and how this information will be incorporated into the implementation of the surveillance program.

10 CFR 70.64 (a)(8) requires that the design of items relied on for safety must provide for adequate inspection, testing, and maintenance, to ensure their availability and reliability to perform their function when needed. NUREG 1718 Section 15.3.4.3.B.i states that a license application is acceptable if it adequately addresses “the surveillance monitoring function, its responsible organization, and the conduct of surveillance/monitoring at specified frequencies to measure the degree to which safety functions or safety controls meet performance specifications. This activity is used in setting preventive maintenance frequencies for safety controls and the determination of performance trends for safety controls. How results from incident investigations...and identified root causes are used to modify the affected maintenance function and eliminate or minimize the root cause from recurring should be addressed. For surveillance tests that can be done only while equipment is out of service, proper compensatory measures should be prescribed.”

NUREG 1718 Section 15.3.4.3.B.iii states that a license application is acceptable if it adequately addresses “a description of the preventative maintenance function that contains a commitment to conduct preplanned and scheduled periodic refurbishing or

partial or complete overhaul for the purpose of providing reasonable assurance that the reliability and availability goals for the IROFS will continue to be met even with unplanned outages. This activity includes the results of the surveillance/monitoring component of maintenance. Instrument calibration and testing should be addressed as part of this component.”

PS-I&C-17

LA Section 15.3

Incorporation of Surveillance Results into Basis of Instrument Settings

Identify the programs and methods that will be implemented to coordinate the revision of instrument and control calibration ranges and setpoints for IROFS based on data from incident investigations and surveillance results that may indicate required changes to setpoints or an establishment of more appropriate instrument calibration surveillance intervals.

10 CFR 70.64 (a)(8) requires that the design of items relied on for safety must provide for adequate inspection, testing, and maintenance, to ensure their availability and reliability to perform their function when needed.

10 CFR 70.62 (d) requires that management measures shall be established to ensure compliance with the performance requirements of Section 70.61. The management measures shall ensure that engineered and administrative controls and control systems that are identified as items relied on for safety are designed, implemented, and maintained, as necessary, to ensure that they are available and reliable to perform their function when needed, to comply with the performance requirements of Section 70.61.

10 CFR 70.61 (e) requires each engineered or administrative control or control system necessary to comply with paragraphs (b), (c), or (d) of Section 70.61 shall be designated as an item relied on for safety, and that the safety program shall ensure that each item relied on for safety will be available and reliable to perform its intended function when needed and in the context of the performance requirements of section 70.61.

NUREG 1718 Section 15.3.4.3.A states that a license application is acceptable if it adequately addresses “an assessment of whether components and support systems need to be individually maintained to ensure the availability and reliability of specific safety controls.”

NUREG 1718 Section 15.3.4.3.B.i states that a license application is acceptable if it adequately addresses “the surveillance monitoring function, its responsible organization, and the conduct of surveillance/monitoring at specified frequencies to measure the degree to which safety functions or safety controls meet performance specifications. This activity is used in setting preventive maintenance frequencies for safety controls and the determination of performance trends for safety controls. How results from incident investigations...and identified root causes are used to modify the affected maintenance function and eliminate or minimize the root cause from recurring should be

addressed. For surveillance tests that can be done only while equipment is out of service, proper compensatory measures should be prescribed.”

NUREG 1718 Section 11.4.3 states: “The reviewer should find the applicant's instrumentation and control (I&C) systems' design and operation acceptable if they satisfy the requirements listed in Section 11.4.1. ...The I&C systems' design and operation should fulfill the functional requirements determined from the ISA, and the I&C systems should be available and reliable to perform their intended safety function when needed. ...The instrument channels and associated logic should be designed with the following:

- A. Provisions so that I&C system components can be tested periodically for operability and required functional performance
- D. Adequate instrument spans, setpoints, and control ranges to ensure proper monitoring and control of IROFS

PS-I&C-18

LA Section 11.5.1.1.3 and LA Section 15.3

Periodic Surveillance Testing to Verify Proper Functioning of Safety PLCs

Verify that the proposed periodic test surveillance interval selected for the Safety PLCs is consistent with any vendor-established reliability and availability analyses for the particular hardware components selected.

10 CFR 70.64 (a)(8) requires that the design of items relied on for safety must provide for adequate inspection, testing, and maintenance, to ensure their availability and reliability to perform their function when needed.

10 CFR 70.62 (d) requires that management measures shall be established to ensure compliance with the performance requirements of Section 70.61. The management measures shall ensure that engineered and administrative controls and control systems that are identified as items relied on for safety are designed, implemented, and maintained, as necessary, to ensure that they are available and reliable to perform their function when needed, to comply with the performance requirements of Section 70.61.

10 CFR 70.64 (a)(8) requires that the design of items relied on for safety must provide for adequate inspection, testing, and maintenance, to ensure their availability and reliability to perform their function when needed. NUREG 1718 Section 15.3.4.3.A states that a license application is acceptable if it adequately addresses “an assessment of whether components and support systems need to be individually maintained to ensure the availability and reliability of specific safety controls.”

NUREG 1718 Section 15.3.4.3.B.i states that a license application is acceptable if it adequately addresses “the surveillance monitoring function, its responsible organization, and the conduct of surveillance/monitoring at specified frequencies to measure the degree to which safety functions or safety controls meet performance specifications. This activity is used in setting preventive maintenance frequencies for safety controls and the determination of performance trends for safety controls. How results from

incident investigations...and identified root causes are used to modify the affected maintenance function and eliminate or minimize the root cause from recurring should be addressed. For surveillance tests that can be done only while equipment is out of service, proper compensatory measures should be prescribed.”