146. <u>Section 11.4.9, pp. 11.4-24 thru 11.4-26</u>

Explain the philosophy of the fire protection of the final filtration units.

Appendix E of the SRP recommends the use of automatic suppression inside the final filter plenums. The application does not clearly describe the design features that prevent fire events from affecting the HEPA filters.

Response:

Fire protection of the MFFF final HEPA filter system will be provided by using spark arresters to prevent branding of the final filters by hot particles and by dilution of high temperature exhaust streams to prevent prolonged exposure to temperatures above the 400°F maximum filter service temperature.

Spark arresters will be installed in the final HEPA filter boxes, upstream of the first stage of HEPA filters. In addition to the spark arresters, a single stage of high efficiency, fire resistant, pre-filters will be installed downstream of the spark arresters and upstream of the final filters for added protection from hot particles.

An analysis of fire area exhaust flow dilution was performed to determine possible maximum temperatures at the HEPA filter systems during an area fire. The analysis, based on adiabatic mixing, assumed an affected room exhaust temperature of 2300° Fahrenheit (F) and no heat transfer out of the ducting between the fire and the filter systems. The maximum dilution air temperature was also assumed to be 104°F (119°F for the VHD exhaust system) instead of the normal room temperature of 75° to 80°F. The flow rates used in the analysis represent the largest room served by the exhaust systems and are as follows: VHD exhaust system: 130 cfm, HD exhaust system: 3890 cfm, PO exhaust system: 2400 cfm, and MD exhaust system: 6980 cfm. (The largest room served by the PO exhaust system has a maximum fire load of 2 gallons of solvent contained in fully welded pipe and no ignition sources. Therefore, the maximum exhaust temperature from this room cannot reach 2300°F. Therefore, the mixed airflow to the filters will not exceed 400°F. This conclusion will be demonstrated in the ISA.) Possible adjacent areas participating in the fire were also considered. The analysis concluded that the diluted flow temperature for any of the four MFFF HEPA filter systems will not exceed the HEPA filter continuous exposure temperature of 400°F.

Other measures to protect the HEPA filter systems include:

- Locating the filter systems as far as practical from the postulated fires
- Multiple separate filter housings and separation of redundant filter system trains
- Automatic fire dampers, in the MD exhaust systems serving the C2 areas
- Manual fire isolation dampers in the HD exhaust and the PO exhaust systems serving the C3 and PC areas
- Manual fire isolation valves in the VH exhaust system serving the gloveboxes

- No ignition sources within the filter housing
- No combustible materials within the filter housing
- Limited combustible materials in the filter housing rooms
- Temperature monitoring of the exhaust air stream
- Fire detection and temperature monitoring in process rooms.

A discussion related to soot loading is provided in the response to Question 148. A discussion related to automatic suppression (sprinklers) is provided in the response to Question 59.

Action:

None

147. Section 11.4.9, pp. 11.4-24 thru 11.4-26

Describe the in-place testing provisions applicable to HEPA filters located at the glovebox interfaces and at C3 boundaries.

Regulatory Guide 3.12, "General Design Guide for Ventilation Systems of Plutonium Processing and Fuel Fabrication Plants," states that HEPA filters should be tested after installation. Section 11.4.9.1 describes in-place testing provision designs for the final HEPA filter stages, but does not indicate that HEPA filters located at the glovebox interfaces and C3 boundaries are designed to accommodate in-place testing after installation. In-place testing is important to ensure that installation has been performed properly to ensure correct seating of HEPA filters and frames. Small seating defects can result in loss of design particulate removal efficiencies.

Response:

Gloveboxes are provided with two stages of HEPA filtration on both the normal inlet and the normal exhaust, and at least one stage is testable. One filter stage is outside of the glovebox; the other stage is inside the glovebox. The filter design for the gloveboxes includes one bag-out type filter housing on the inlet and exhaust with in place testing ports on the filter housing, to check for proper seating of the filter. This filter housing will be on the external stages only, for access purposes. The HEPA filter stage on the inside of the glovebox will not be tested.

HEPA filters at the C3 boundaries will have the same provisions as above for testing.

These filters are provided to prevent plutonium oxide from contaminating the HVAC exhaust ducts and are not classified as principal SSCs, as these filters are not credited in the normal release or accident dose analysis (although they would provide a decontamination factor of ~0.01 if credited).

Action:

Clarify in the CAR that these filters are not principal SSCs.

148. Section 11.4.9.2, pp. 11.4-25 thru 11.4.26

Provide the design soot loading analysis to support the functioning of the HEPA filter units during fire scenarios. Provide a basis for assuming that the ventilation system can withstand credible explosion events.

Regulatory Guide 3.12, "General Design Guide for Ventilation Systems of Plutonium Processing and Fuel Fabrication Plants," states that ventilation systems should be designed to withstand any credible fire and explosion and continue to act as confinement barriers. In Section 11.4.9.2, the application provides a brief summary of the soot loading analysis used to show that HEPA filters can withstand the loadings from soot in internal fire scenarios. No discussion is provided on hypothetical explosion events.

Response:

Soot Loading:

A soot loading analysis was performed to address the final HEPA filter system soot loading produced by a fire in the fire area with the largest combustible load in rooms exhausted by the HD exhaust system (C3 process area), PO Exhaust system (PC process area), and MD exhaust system (C2 process area).

The analysis used the following assumptions:

- No credit was taken for intermediate filters, spark arresters, and prefilters.
- The soot handling capacity of the HEPA filters will increase significantly when the volumetric flow through the filter is reduced due to soot loading. For a flow reduction of 20%, the soot loading capacity for a HEPA filter is estimated to increase by a factor of 5. (Washington Group, 2001).
- Soot loading capacity, at design air flow, of the HEPA filters equals the loading estimated from the Ballinger correlation (Ballinger, 1988).
- All filters in the exhaust system are utilized.
- Combustion efficiency of a compartment fire is 45%.

A soot loading analysis was not performed for the VH exhaust system (which serves the gloveboxes) final filters because it is assumed that a glovebox fire would involve the gloves, which would breach the glovebox barrier and involve the HD exhaust system. In this event, the glovebox that is involved in the fire would be isolated from the VH exhaust system and, if necessary, the exhaust flow could be diverted to the redundant filter train after isolation.

The C3 process fire area with the largest combustible loading is Room B-264, Cladding and Decladding. For Room B-264, fire loading and material composition is concentrated in the process units (i.e., gloveboxes) in the area, with approximately 75% of the combustible loading in the area residing in the process units.

The combustible loading that resides within the process units (which is assumed to be 75% of the combustible loading of the process area) is assumed to be comprised of the following constituents:

35% - Polycarbonate (in the form of glovebox windows)
30% - Polymethyl methacrylate (in the form of radiological shielding material)
15% - Polyethylene (in the form of bagport sleeves and radiological shielding material)
15% - Polychloroprene (i.e., neoprene) (in the form of window joint seals and glovebox gloves)
5% - Polyvinyl chloride (in the form of cable insulation)

The remaining 25% of the combustible loading in a C3 process area is assumed to be composed of polyvinyl chloride in the form of light covers, fire detectors, cable insulation, etc.

The C3 process fire area with the largest combustible loading is Room B-264, Cladding and Decladding. Based on the tables in the Preliminary Fire Hazards Analysis (PFHA), this fire area has a floor area of 6,431 square feet and a fire load density of 81,808.5 BTU/ft^2, resulting in a total fire load of approximately 5.26 x 10^8 BTU. The soot yield is determined in accordance with the combustible load and is shown in the following table:

Material	Percentage of material in the area	Fire Load Contribution (BTU) (Percentage x 5.26E+8)	Approximate Heat of Combustion (Btu/lb)	Weight of material participating in fire in pounds (45% of material participating per Assumption)	Soot yield %	Soot weight produced (pounds)
Polyvinyl chloride	28.75%	1.512E+8	7730	8802	12%	1056
Polycarbonate	26.25%	1.381E+8	13346	4656	11%	512
Polymethyl methacrylate	22.5%	1.184E+8	11473	4644	2%	93
Polyethylene	11.25%	5.918E+7	20026	1330	17%	226
Polychloroprene	11.25%	5.918E+7	11542	2307	17%	392
Total	100%	5.26E+8		21739		2279

The actual amount of soot reaching the final HEPA filter system is determined by applying the following equation from Ballinger:

$$1 - E = \mathrm{Exp}\ \{-4y \times L / (v_g \times D)\}\ \text{(Ballinger)}$$

Where E = deposition factor of smoke in the duct, y = deposition velocity of smoke, vg = air flow velocity, L = duct length and D = duct diameter. The soot deposited in the duct system is subtracted from the soot load entering the duct system and the result is the soot loading reaching the HEPA filter system.

The amount of soot that the HEPA filters are capable of handling is predicted by the simplified Ballinger correlation:

$$\Delta P = \Delta P_0 + 0.14 M_a + 1.6x10^{-4} M_a^2$$

Where:

ΔP =Differential Pressure across the filters at failure in mm WG (10.5 in WG)

ΔP_0 = Differential Pressure across the filters at change out in mm WG (1.8 in WG)

M_a =Amount of soot loaded on filter in grams.

The soot loading capability of the HEPA filters was estimated from the Ballinger correlation and was determined to be 4.08 kg/filter for a 24-inch x 24-inch x 12-inch HEPA filter rated at 2000 cfm. For the C3 area with largest fire load (Room B-264), the soot loading on the HEPA filters is approximately 3.5 kg/filter, which was determined by dividing the soot loading reaching the HEPA filter system, from above, by the total number of filters. This quantity of soot is within the capacity of the HEPA filters.

Similar analyses were performed for the filters serving the MD exhaust system and the PO exhaust system. The results are summarized as follows:

For the MD exhaust system, the filter soot loading is 1.6 kg/filter.

For the PO exhaust system, the filter soot loading is 0.67 kg/filter.

Other measures to protect the HEPA filter systems are:

- Soot loading capacity of the spark arresters and the prefilters will significantly reduce the soot load on the final filters.
- Intermediate filters and spark arresters are provided at the C3 room boundaries, ahead of the final HEPA filter in the C3 exhaust system, which will reduce the amount of soot reaching the final filters.

Subsequent to submittal of the CAR, revisions have been made to the design that reduce the fire load in the design basis room and increase the number of HEPA filters. The ability of the final HEPA with respect to soot loading will be demonstrated in the ISA.

References:

Ballinger, M. Y., et al., 1988. "Aerosols Released in Accidents in Reprocessing Plants", Nuclear Technology, Vol. 81, pp 278 – 292, May 1988

Washington Group, 2001. PDCF HEPA Filter/Sand Filter Alternatives Analysis Study, Contract No. DE-AC02-99CH10903, Project No. 79065.001, January 19, 2001

Hypothetical Explosion Events:

Hypothetical explosion events and their associated consequences are discussed in detail in Sections 5.5.2.4 and 5.5.3.5, respectively, of the MFFF Construction Authorization Request. The discussion in Section 5.5.3.5 concludes that the "MFFF processes are designed to preclude explosions through the use of highly reliable principal SSCs and administrative controls, the simultaneous failure of which is highly unlikely." Table 5.5-19 identifies the principal SSCs and their function in the prevention of explosion events. Therefore, there are no credible explosion events that can adversely impact the ventilation systems.

The design basis for potential explosions in the laboratory is to ensure that they do not impact process operations (from a safety perspective), and to ensure that the ventilation system can mitigate any direct radioactive material release from the laboratory. This commitment will be demonstrated in the ISA. Calculations will be performed to demonstrate that a laboratory explosion and the resultant pressure waves will not impact process operations, and to demonstrate the effectiveness of the ventilation system following a laboratory explosion.

Action:

For clarification, the first sentence of the fourth paragraph of Section 11.4.11.1 will be revised to read "The principal ventilation SSCs, including final filters, are designed to prevent explosions (in conjunction with other principal SSCs) and remain operational after facility fires."

149. <u>Figure 11.4-11, p. 11.4-57</u>

Clarify the design capacities for the High Depressurization Exhaust System.

Figure 11.4-11 indicates that for the High Depressurization Exhaust System there are two 100 percent capacity filtration trains each with 9 filtration units each having the capacity of about 6,000 CFM (2 by 3 cells, assuming each cell is rated for 1000 CFM, a standard HEPA filter size). The total capacity of each train would be 54,000 CFM. However, the figure also shows a design inlet capacity of 77,870 CFM. There appears, therefore, to be a discrepancy in the filtration train ratings and the total design airflow requirements. A similar discrepancy also exists for the Medium Depressurization Exhaust System, where the design flow into the filtration units is 116,870 CFM and the total capacity of the filtration units is 66,000 CFM, assuming standard 1000 CFM HEPAs are used. Section 11.4.2.5 of the application indicates that there is sufficient capacity in the filtration units to allow units to be shutdown for maintenance and still maintain design flow.

Response:

The following general design information is provided:

The number of HEPA filters were originally based on using a size 8 HEPA filter rated at 2000 cfm and 1.3 inches water gauge pressure drop. This rating was taken from DOE-STD-3020-97 and ASME AG-1. 1850 cfm per filter was used when selecting the number of filters required. As an example, under this rating, the final filter units for HDE are rated at 6 x 1,850 or 11,100 cfm, each, and nine filter units would have a capacity of 99,900 cfm.

No manufacturer currently offers a certified nuclear grade HEPA that has the capacity of a size 8 filter. The highest capacity is a size 7 rated at 1,500 cfm. The 1,500-cfm capacity rating is acceptable even though the filter exceeds the 5-foot per minute filter media velocity required by DOE-STD-3020-97 and ASME AG-1, based on a DOE exception for SRS (based on manufacturer input).

DCS has been advised that ASME AG-1 may be revised to delete the 5 fpm filter velocity requirement, making an exception unnecessary for this filter. As part of final design, if a revision to AG-1 is not made, DCS will substantiate the DOE exception or a filter rating of 1,250 cfm will be used and the final filter boxes resized accordingly.

The rating of the VHD filter units, based on the size 7 filter (1 filter wide by 2 filters high), as described above, is 3,000 cfm for a total installed capacity in two filter units of 6,000 cfm providing 100% redundancy to serve the system design flow rate of 2,300 cfm.

The rating of the HDE filter units, based on the size 7 filter (2 filters wide by 3 filters high), as described above, is 9,000 cfm for a total installed capacity in 18 filter units of 162,000 cfm providing 100% redundancy to serve the system design flow rate of 78,000 cfm.

The rating of the MDE filter units, based on the size 7 filter (3 filters wide by 3 filter high), as described above, is 13,500 cfm for a total installed capacity in 10 filter units 135,000 cfm providing two spare filter units to serve the system design flow rate of 101,000 cfm.

Action:

None

150. Section 11.5.2.3.1, p. 11.5-4

Provide justification for using only one 7-day fuel tank for the emergency diesel generators (EDGs) and why a larger tank size is not needed for the limiting design basis event. Also, explain why this decision is consistent with IEEE Std 308-1991, "IEEE Standard Criteria for Class 1E Power Systems for Nuclear Generating Stations."

On page 11.5-14 of the application, DCS states that the fundamental design of the emergency Alternating Current power system is in accordance with IEEE Std 308-1991. In an April 25, 2001, meeting, DCS stated that redundant 7-day fuel tanks were being considered. On page 11.5-15, the application states, "The fuel oil supply tank provides sufficient storage capacity to allow one emergency diesel generator to operate continuously for seven days." This appears to be inconsistent with Section 6.2.5(5)(a) of IEEE Std 308-1991.

Response:

EGF Storage Capacity

The revised configuration of the EGF System consists of two independent sub-systems, each capable of fuel receipt, maintaining the fuel for long-term storage, and the ability to transfer an adequate supply of fuel oil to support its associated Emergency Diesel Generator operating at 100% load for seven days.

This is consistent with IEEE Std 308-1991. The emergency fuel oil storage capacity as defined by ANSI/ANS 59.51-1997 (Section 5.2) and IEEE Std 308-1991 (Section 6.2.5(5)a) will include supply fuel for the *longer* of the following time periods: either (1) seven days, or (2) the time it takes to replenish the fuel supply. A new fuel supply can be obtained and made ready for usage in less than 72 hours, which includes time to verify fuel quality (per ANSI/ASTM D975-94) *prior* to filling the storage tank. Consequently, this requires the maintenance of a minimum of a seven-day emergency fuel oil supply.

Action:

In the next update of the CAR, revise Sections 11.5.2.3.1, 11.5.7.1, 11.9.1.7.2, and 11.9.1.7.3 and Figure 11.9-7 as appropriate to reflect the revised configuration of the fuel oil system.

151. Section 11.5.2.4, p. 11.5-6

Provide a discussion for the MOX communication systems.

Although communication systems have been included as electrical systems in Section 11.5.2.4 of the application, there appears to be no separate, unique discussion in the application for communication systems related to information and acceptance criteria encompassed by Sections 11.3 and 11.4 of the SRP.

Response:

Communications Systems

The MFFF Communications System is not a principal SSC, and the CAR section dealing with communications was presented for information only. The function(s) of the system are to provide voice and data communications throughout the site and to the public exchange. The system does not mitigate the consequences of any accident condition. For this reason, the system is non-IROFS. Power for the communications system equipment will be provided by non-IROFS UPS. The communications system will be designed to normal industry standards EIA/TIA and NFPA.

The communications system for the MFFF provides multiple means of communication for normal operations and maintenance, emergency conditions, and security. These systems will allow communications under all anticipated circumstances during normal and emergency conditions. The trunked radio system and public address system are powered from the essential UPSs that are provided power from the standby diesel generators upon loss of normal power.

Action:

This information will be incorporated into the next update of the CAR.

152. Sections 11.5.2.5, p. 11.5-7; Section 11.6.7, pp. 11.6-12 thru 11.6-14; and Section 15.3, pp. 15-12 thru 15-14

Discuss commitments to maintenance and periodic testing standards for electrical and Instrumentation and Control (I&C) SSCs.

Although there is a commitment to testing in Sections 11.5.2.5, 11.6.7, and 15.3 of the application; there appears to be no commitment (ignoring cross-referenced standards) to specific standards for maintenance and periodic testing for electrical and I&C SSCs (e.g. Institute of Electrical and Electronics Engineers (IEEE) Standard 450; "IEEE Recommended Practice for Maintenance, Testing, and Replacement of Vented Lead-Acid Batteries for Stationary Applications") as mentioned in Sections 11.3 and 11.4 of the SRP.

Response:

Maintenance and Periodic testing of electrical and I&C principal SSCs will be performed at regular intervals to provide the necessary component and systems reliability as required by the ISA such that the principal SSCs meet the design performance criteria. DCS has also committed to a number of industry standards that provide maintenance and testing criteria. At this stage in the design, the ISA process has not been completed, and maintenance and testing requirements from the ISA are not available. The industry standards provide testing, maintenance and inspection criteria that MFFF have made provisions for in the design. The following is a description of these criteria from the standards.

IEEE Std 308-1991 provides guidance on pre-operational equipment tests, pre-operational system tests, and periodic tests. DCS will comply with the guidance provided. IEEE Std 338-1987 provides general considerations and program objectives for periodic surveillance testing programs at nuclear power generating stations. The standard also provides types of tests that should be performed, test methods and criteria for the establishment of test intervals, and changing those intervals. DCS MFFF will comply with the broad guidance and spirit of the standard recognizing that there may be specifics that are applicable to a nuclear power generating station that would not be applicable to a fuel processing facility (e.g., safety injection signal testing). However, a surveillance testing program will be instituted that is in keeping with the guidance of IEEE Std 338-1987. IEEE Std 765-1995 provides guidance for surveillance, periodic and pre-operational tests on the preferred power supply and associated circuits. DCS will follow the guidance outlined in the standard; however, it should be noted that the preferred power supply is the normal source of power for the MFFF. IEEE Std 450-1995 provides maintenance inspection criteria and time frames for batteries. It also proposes corrective actions and provides test schedules and descriptions. DCS will follow the guidance of the standard when establishing maintenance and test schedules for the station batteries. IEEE Std 387-1995, Section 6.5.1, requires a separate preventive maintenance, inspection, and testing program be established for the DG and all supporting systems based on the manufacturer's recommendations. It also lists specific portions of the unit for which a program is required. Section 7 deals with all aspects of site testing, acceptance, pre-operational and periodic. Specific tests are called out in each area. DCS will comply with the guidance presented in the standard.

Other standards reviewed, in general, deferred to the guidance of IEEE Std 308 and IEEE Std 338 for periodic and surveillance testing requirements. DCS MFFF will rely on manufacturer's recommendations for maintenance activities and schedules unless specific guidance is presented in the standards mentioned above.

Action:

None

153. Sections 11.5.6 and 11.5.7, pp. 11.5-13 thru 11.5-16

Discuss DCS's lack of commitment to IEEE Standard 944-1986, "IEEE Recommended Practice for the Application and Testing of Uninterruptible Power Supplies for Power Generating Stations."

Section 11.3 of the SRP recommends that information be provided to determine if the design basis adequately addresses the functional requirements for the system. Per Section 11.4.2.2 of the SRP, electrical systems should be available and reliable and designed with specific considerations such as those contained in IEEE Standard 944.

Response:

IEEE Std 944-1986, "IEEE Recommended Practice for the Application and Testing of Uninterruptible Power Supplies for Power Generating Stations," provides general information on the application requirements, procurement requirements, and testing requirements for UPS systems.

DCS will comply with the guidance of the standard as the UPS design and procurement activities progress.

Action:

None

154. <u>Sections 11.5.6 and 11.5.7, pp. 11.5-13 thru 11.5-16</u>

Discuss DCS's lack of commitment to IEEE Standard 946-1985, "IEEE Recommended Practice for the Design of Safety-Related DC Auxiliary Power Systems for Nuclear Power Generating Stations."

Section 11.3 of the SRP recommends that information be provided to determine if the design basis adequately addresses the functional requirements for the system. Per Section 11.4.2.2 of the SRP, electrical systems should be available and reliable and designed with specific considerations such as those contained in IEEE Standard 946.

Response:

IEEE Std 946-1992, "IEEE Recommended Practice for the Design of DC Auxiliary Power Systems for Generating Stations," provides general guidance on the design and application of DC auxiliary power systems. DCS will comply with the guidance of the standard in the design of the MFFF DC power system. The 1992 revision of the standard will be used, as it is the current revision of record.

The significant differences between the 1985 version of the standard and the 1992 revision are the following:

- Section 4.1 – A requirement has been added that a DC system that performs a safety function shall meet the requirements of IEEE Std 603-1991 and IEEE Std 308-1991, and shall be qualified in accordance with IEEE Std 627-1980.
- Section 4.5 – A requirement has been added to separate DC power system cables and equipment to the same extent that AC power system cables and equipment are separated.
- Section 5.2 – This section points out that consideration should be given to providing additional design margin so that the battery will be capable of performing its design function with one or more cells removed.
- Section 6.2 – Explicit guidance is provided for sizing the charger for the combination of the largest continuous load and the largest non-continuous load.
- Section 6.5.3 – This section has been added to address load sharing between parallel chargers.
- Section 7.1 – The importance of low inductance in the DC system is pointed out, a note added to point out potential problems with fractional minute loads and it is pointed out that time-current curves should be based on DC not AC.
- Section 7.4.2 – This section has been added to address DC system grounds and ground detection.

- Section 7.4.3 – This section has been added to address DC bus undervoltage alarms.
- Section 7.5.4 – This section has been added to address point out that the filtering of electrical noise should be considered.
- Section 7.8 – This section requires that cable, field splices and connections be qualified in accordance with IEEE Std 383-1974.
- Section 7.9.3 – This section provides detail on the contribution of DC motors to short circuit current. The previous version of the standard maintained that the contribution was insignificant.
- Two Annexes have been added. Annex C addresses the effects of grounds on the operation of DC power systems. Annex D addresses battery charger short circuit contribution.

Action:

None

155. <u>Section 11.5.6.1, p.11.5-13</u>

Discuss compliance with IEEE Standard 665-1987, "Guide for Generating Station Grounding." Discuss how the DCS commitment to IEEE Standard 1050-1996, "Guide for Instrumentation and Control Equipment Grounding in Generating Stations," meets the guidance provided in Regulatory Guide 1.180, "Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems."

DCS has committed to IEEE Standard 142-1991, "Recommended Practice for Grounding of Industrial and Commercial Power Systems," which is related to IEEE Standard 665-1987. DCS has also committed to IEEE Standard 1050-1996. The NRC staff, in Regulatory Guide 1.180, has endorsed IEEE Standard 1050-1996 with exceptions.

Per Section 11.3 of the SRP, information is recommended to determine if the design basis adequately addresses the functional requirements for the system. Per Sections 11.4.2.2 and 11.4.3.2 of the SRP, electrical and instrumentation and control systems should be available and reliable and designed with specific considerations such as those contained in IEEE Standards 665 and 1050 and Regulatory Guide 1.180.

Response:

IEEE Std 665-1995, "Guide for Generating Station Grounding," provides design objectives and design criteria that are generally accepted in the utility industry as contributing to effective grounding systems for personnel safety and equipment protection in generating stations. Although the Question referenced the 1987 version of the standard, 1995 is the latest revision and will be discussed here. DCS has committed to following the guidelines of IEEE Std 142-1991, "IEEE Recommended Practice for Grounding of Industrial and Commercial Power Systems," which is appropriate for an industrial facility such as the MFFF. IEEE Std 142-1991 provides guidance on system grounding, equipment grounding, static and lightning protection grounding, connections to earth and sensitive electronic equipment grounding. IEEE Std 665-1995 is related to IEEE Std 142-1991 in that Std 665 references Std 142. The techniques for grounding equipment and structures are compatible between the two documents. Both documents, while providing guidance on lightning protection grounding, appropriately reference NFPA 780, *Lightning Protection Code* on this subject.

IEEE Std 665-1991 also provides guidance in the sizing of grounding conductors and ground grid design. Regulatory Guide 1.180 position 2 endorses the portions of IEEE Std 665-1995 that are referenced in IEEE Std 1050-1996. Specifically, IEEE Std 1050-1996 defers to IEEE Std 665 in the areas of grounding systems related to lightning, station service power and equipment. DCS will follow the guidance of IEEE Std 655-1995 for lightning protection, station service power and equipment grounding.

Regulatory Guide 1.180 position 2 also endorses IEEE Std 1050-1996 with the exception that a clarification was made in Section 4.3.7.4, Radiative Coupling, to indicate that the field strength of propagating electromagnetic waves is inversely proportional to the distance from the source of radiation not the square of the distance. DCS will appropriately factor this information into the use of the standard.

The other Regulatory Positions of Regulatory Guide 1.180 require:

- Establishment of an electromagnetic compatibility program for safety related instrumentation and control systems (Pos. 1)
- Acceptable test criteria as referenced in MIL-STD 461 regarding susceptibility and emissions are identified (Pos. 3)(note that criteria from both revisions C and D are referenced for user option)
- Test methods from MIL-STD-462D are identified along with acceptance values for the various tests (Pos. 4)
- Test methods from MIL-STD-462 are identified along with acceptance values for the various tests (Pos. 5)
- The SWC practices described in IEEE Std C62.41-1991, *IEEE Recommended Practice on Surge Voltages in Low-Voltage AC Power Circuits* and IEEE Std C62.45-1992, *IEEE Guide on Surge Testing for Equipment Connected to Low-Voltage AC Power Circuits* are endorsed and typical environmental conditions for power surges in a nuclear power plant are provided (Pos. 6).

DCS will follow the requirements of Regulatory Guide 1.180 regarding EMC required testing and acceptance criteria for safety related instrumentation and control systems.

Action:

None

156. <u>Section 11.5.7.1, p. 11.5-14</u>

Discuss any significant difference (applicable to MOX) between IEEE Standard 387-1995, "IEEE Standard Criteria for Diesel Generator Units Applied as Standby Power Supplies for Nuclear Power Generating Stations," and the 1984 version of this standard. Discuss how the DCS commitment to IEEE Standard 387-1995 meets the guidance provided in Revision 3 of Regulatory Guide (RG) 1.9, "Selection, Design, and Qualification of Diesel-Generator Units Used as Standby (Onsite) Electrical Power Systems at Nuclear Power Plants."

DCS has committed to IEEE Standard 387-1995. The NRC staff, in Revision 3 to Regulatory Guide 1.9, endorses IEEE Standard 387-1984. Some, but not all, of the Regulatory Guide 1.9, Revision 3, guidance has been incorporated in IEEE Standard 387-1995.

Per Section 11.3 of the SRP, information is recommended to determine if the design basis adequately addresses the functional requirements for the system. Per Section 11.4.2.2 of the SRP, electrical systems should be available and reliable and designed with specific considerations such as those contained in IEEE Standard 387 and Regulatory Guide 1.9.

Response:

The 1995 revision of IEEE Std 387 includes the requirements of the 1984 version and provides additional detail over that of the previous revision of the standard in the following areas:

(a) Defining specific qualification requirements

(b) Clarifying scope and scope diagram

(c) Providing requirements for no-load and light-load operation, since extended operation under these conditions may be detrimental to unit performance

(d) Expanding factory production testing and site testing criteria

(e) Updating specific surveillance requirements

(f) Providing guidance for test parameters

(g) Providing guidance for reliability program elements

The 1995 revision also incorporates the periodic testing requirements described in IEEE Std 749-1983, "IEEE Standard for Periodic Testing of Diesel Generator Units Applied as Standby Power Supplies in Nuclear Power Generating Stations," which has been withdrawn. IEEE 387-1995 is a more modern and comprehensive standard that addresses the Commissions exceptions identified in Regulatory Guide 1.9, Rev. 3. The following is a summary of the differences between the two revisions of the standards including the clarification provided in Regulatory Guide 1.9, Rev. 3.

Regulatory Guide 1.9, Rev. 3 found that conformance with the guidelines in IEEE Std 387-1984 acceptable to the NRC staff for satisfying the Commission's regulations with respect to design, qualification, and periodic testing of diesel generator units used as onsite electric power systems for nuclear power plants subject to the following:

> 1.1 Section 1.2, "Inclusions," of IEEE Std 387-1984 should be supplemented to include diesel generator auto controls, manual controls, and diesel generator output breaker.

Section 1.1.2 of the 1995 version of the standard lists the following items as being included for site testing purposes:

a) The AC and DC power distribution system, which includes

   1) Circuits conveying ac power from the diesel generator terminals up to and including the main disconnect device.

   2) Circuits for conveying ac or dc power to the diesel generator units and associated controls

   3) DC power supplies, if dedicated to the diesel generator unit.

b) The remote and local control, protection, and surveillance systems, which include

   1) Devices for automatic and manual starting
   2) Devices for load shedding and sequencing
   3) Remote devices for the protection of the diesel generator unit and its auxiliary equipment
   4) Synchronizing equipment
   5) Field flashing devices

> 1.2 When the characteristics of the required emergency diesel generator loads are not accurately known, such as during the construction permit stage of design, each emergency diesel generator unit of an onsite power supply system should be selected to have a continuous load rating (as defined in Section 3.7.1 of IEEE Std 387-1984) equal to the sum of the conservatively estimated loads (nameplate) needed to be powered by that unit at any one time plus a 10 to 15 percent margin. In the absence of fully substantiated performance characteristics for mechanical equipment such as pumps, the electric motor drive ratings should be calculated using conservative estimates of these characteristics, e.g., pump runout conditions and motor efficiencies of 90 percent or less and power factors of 85 percent or lower.

Annex A of the 1995 standard provides a method for establishing a load profile for a diesel generator unit. The information required to properly size the unit is detailed in this section.

> 1.3 At the operating license stage of review, the predicted loads should not exceed the continuous rating (as defined in Section 3.7.1 of IEEE Std 387-1984) of the diesel generator unit.

Section 4.1.2 (b) requires that the diesel be capable of starting, accelerating, and being loaded with the design load within the time required by the equipment specification. DCS will specify a machine with margin available above the known loads to allow for some future growth.

1.4 Section 5.1.2, "Mechanical and Electrical Capabilities," of IEEE Std 387-1984 pertains, in part, to the starting and load-accepting capabilities of the diesel generator unit. In conformance with Section 5.1.2, each diesel generator unit should be capable of starting and accelerating to rated speed, in the required sequence, all the needed engineered safety feature and emergency shutdown loads. The diesel generator unit design should be such that at no time during the loading sequence should the frequency decrease to less than 95 percent of nominal nor the voltage decrease to less than 75 percent of nominal (a larger decrease in voltage and frequency may be justified for a diesel generator unit that carries only one large connected load). Frequency should be restored to within 2 percent of nominal in less than 60 percent of each load-sequence interval for step load increase and in less than 80 percent of each load-sequence interval for disconnection of the single largest load, and voltage should be restored to within 10 percent of nominal within 60 percent of each load-sequence time interval. (A greater percentage of the time interval may be used if it can be justified by analysis. However, the load-sequence time interval should include sufficient margin to account for the accuracy and repeatability of the load-sequence timer.) During recovery from transients caused by the disconnection of the largest single load, the speed of the diesel generator unit should not exceed the nominal speed plus 75 percent of the difference between nominal speed and the over-speed trip setpoint or 115 percent of nominal, whichever is lower. Furthermore, the transient following the complete loss of load should not cause the speed of the unit to attain the overspeed trip setpoint.

The 1995 version of the standard does not have specific values for voltage and frequency variation. Test results are to be within specified limits. DCS will use the values in position 1.4 as acceptance criteria.

1.5 Emergency diesel generator units should be designed to be testable as described in Regulatory Position 2. The design should include provisions so that testing of the units will simulate the parameters of operation (manual start, automatic start, load sequencing, load shedding, operation time, etc.), normal standby conditions, and environments (temperature, humidity, etc.) that would be expected if actual demand were to be placed on the system. If prewarm systems designed to maintain lube oil and jacket water cooling at certain temperatures or prelubrication systems or both are normally in operation, this would constitute normal standby conditions for that plant.

The units should be designed to automatically transfer from the test mode to an emergency mode upon receipt of emergency signals.

This position is consistent with IEEE Std 387-1995. Sections 4.5.1.4 and 4.5.1.5 address placing the governor and voltage regulator in the proper mode automatically when the diesel is required to operate automatically. The tests described above are periodic tests described in the standard.

1.6 Design provisions should include the capability to test each emergency diesel generator unit independently of the redundant units. Test equipment should not cause a loss of independence between redundant diesel generator units or between diesel generator load groups. Testability should be considered in the selection and location of instrumentation sensors and critical components (e.g., governor, starting system components). Instrumentation sensors should be readily accessible and designed so that their inspection and calibration can be verified in place. The overall design should include status indication and alarm features.

Section 4.3 of the standard "Interactions" addresses independence between units; however, adherence to IEEE Std 338 would prevent a loss of independence between units while testing also. See the response to Question 152. Inspection, testing, and calibration will be factored into the location and design of sensors.

> 1.7 Section 5.5.3.1, "Surveillance Systems," of IEEE Std 387-1984 pertains to status indication of diesel generator unit conditions. The guidance in this section should be supplemented as follows:
>
> 1.7.1 A surveillance system should be provided with remote indication in the control room for displaying emergency diesel generator unit status, i.e., under test, ready-standby, lockout. A means of communication should also be provided between diesel generator unit testing locations and the main control room to ensure that the operators are cognizant of the status of the unit under test.

Section 4.5.3 of the standard addresses the minimum modes that are surveyed by the surveillance system. Table 1, Design and Application Considerations, lists communications between the diesel generator and the control room as one item that should be considered in the design and application of the unit. This is also referred to in IEEE Std 338 as a component of periodic surveillance testing.

> 1.7.2 In order to facilitate trouble diagnosis, the surveillance system should indicate which of the emergency diesel generator protective trips has been activated first.

Section 4.5.3.3 of the standard addresses systems of the diesel generator that must have sufficient mechanical and electrical instrumentation to survey the variables required for successful operation and to generate the abnormal, pre-trip and trip signals required for alarm of such conditions. The standard does not require "first out" annunciation or a specific data monitoring method. However, with digital monitoring equipment, time sequencing of alarms and events is more of an industry standard practice today. DCS will factor this into the system design requirements.

> 1.8 Section 5.5.4, "Protection," of IEEE Std 387-1984, which pertains to bypassing emergency diesel generator protective trips during emergency conditions, should be supplemented as follows:
>
> The emergency diesel generator unit should be automatically tripped on an engine overspeed and generator-differential over-current. All other diesel generator protective trips should be handled in one of two ways:
>
> (1) a trip should be implemented with two or more measurements for each trip parameter with coincident logic provisions for trip actuation, or (2) a trip may be bypassed under accident conditions provided the operator has sufficient time to react appropriately to an abnormal diesel generator unit condition. The design of the coincident logic trip circuitry should include the capability for indication of individual sensor trips. The design of the bypass circuitry should include the capability for (1) testing the status and operability of the bypass circuits, (2) alarming in the control room for abnormal values of all bypass parameters (common trouble alarms may be used), and (3) manually resetting the trip bypass function. Capability for automatic reset is not acceptable.
>
> Section 5.5.4(2) of IEEE Std 357-1984, on retaining all protective devices during emergency diesel generator testing, does not apply to a periodic test that demonstrates diesel generator system response under simulated accident conditions per Regulatory Positions 2.2.5, 2.2.6, and 2.2.12.

This section content is essentially the same in the new standard. The references to bypass circuitry are not applicable to the MFFF. DCS agrees that a simulated accident signal should cause the unit to respond as if an accident were present (i.e., only the differential and overspeed trips would remain active unless multiple sensors were used as stated above).

2. DIESEL GENERATOR TESTING

Section 3, "Definitions," Section 6, "Testing," and Section 7, "Qualification Requirements," in IEEE Std 387-1984 should be supplemented as discussed below.

2. 1 Definitions

Figure 1 illustrates those components and systems that should be considered to be within the emergency diesel generator boundary for purposes of evaluating failures. Systems that provide support to the emergency diesel generator and perform other plant functions are shown outside this boundary. IEEE Std 387-1984 and ANSI/ASME OM-16 provide similar definitions of components and system boundaries and may also be used as guidance.

The following definitions are applicable to the positions of this regulatory guide that address testing, record keeping, and reporting of emergency diesel generator performance.

Start demands: All valid and inadvertent start demands, including all start-only demands and all start demands that are followed by load-run demands, whether by automatic or manual initiation. A start-only demand is a demand in which the emergency generator is started, but no attempt is made to load the emergency diesel generator. See "Exceptions" below.

Start failures: Any failure within the emergency generator system that prevents the generator from achieving specified frequency (or speed) and voltage classified as a valid start failure. (For the monthly surveillance tests, the emergency diesel generator can be brought to rated speed and voltage in a time that is commended by the manufacturer to minimize stress an wear. Similarly, if the generator fails to reach rated speed and voltage in the precise time required by technical specifications, the start attempt is not considered a failure if the test demonstrated that the generator would start and run in an emergency.) See "Exceptions" below. Any condition identified in the course of maintenance inspections (with the emergency diesel generator in the standby mode) that would definitely have resulted in a start failure if a demand had occurred should be counted as a valid start demand and failure.

Load-run demands: To be valid, the load-run attempt must follow a successful start and meet one of the following criteria. See "Exceptions" below.

- A load-run of any duration that results from a real (i.e., not a test) automatic or manual signal.
- A load-run test to satisfy the plant's load and duration test specifications.
- Other operations (e.g., special tests) in which the emergency diesel generator is planned to run for at least 1 hour with at least 50 percent of design load.

Load-run failures: A load-run failure should be counted when the emergency diesel generator starts but does not pick up load, and run successfully. Any failure during a valid load-run demand should be counted. See "Exceptions" below. (For monthly surveillance tests, the emergency diesel generator can be loaded at a rate that is recommended by the manufacturer to minimize stress and wear. Similarly, if the generator fails to load in the precise time required by technical specifications, the load-run attempt is not considered a failure if the test demonstrated that the generator would load and run in an emergency.) Any condition identified in the course of maintenance inspections (with the emergency diesel generator in the standby mode) that definitely would have resulted in a load-run failure if a demand had occurred should be counted as a valid load-run demand and failure.

Exceptions: Unsuccessful attempts to start or load-run should not be counted as valid demands or failures when they can be definitely attributed to any of the following:

- Any operation of a trip that would be bypassed in the emergency operation mode (e.g., high cooling water temperature trip).
- Malfunction of equipment that is not required to operate during the emergency operating mode (e.g., synchronizing circuitry).
- Intentional termination of the test because of alarmed or observed abnormal conditions (e.g., small water or oil leaks) that would not have ultimately resulted in significant emergency generator damage or failure.
- Component malfunctions or operating errors that did not prevent the emergency diesel generator from being restricted and brought to load within a few minutes (i.e., without corrective maintenance or significant problem diagnosis).
- A failure to start because a portion of the starting system was disabled for test purposes if followed by a successful start with the starting system in its normal alignment.

Each diesel generator valid failure that results in the emergency diesel generator being declared inoperable should be counted as one demand and one failure. Exploratory tests during corrective maintenance or preventive maintenance should not be counted as demands or failures. However, the successful test that is performed to declare the emergency diesel generator operable should be counted as a demand.

DCS accepts the definitions listed above.

2.2 Test Descriptions

The following test descriptions are to be used in conjunction with the pre-operational and surveillance testing described in Table 1. The licensee should have detailed procedures for each test described here. The procedures should identify special arrangements or changes in normal system configuration that must be made to put the emergency diesel generator under test. Jumpers and other nonstandard configurations or arrangements should not be used subsequent to initial equipment startup testing.

2.2.1 Start Test: Demonstrate proper startup from standby conditions, and verify that the required design voltage and frequency is attained. For these tests, the emergency diesel generator can be slow-started and reach rated speed on a prescribed schedule that is selected to minimize stress and wear.

2.2.2 Load-Run Test: Demonstrate 90 to 100 percent of the continuous rating of the emergency diesel generator, for an interval of not less than 1 hour and until temperature equilibrium has been attained. This test may be accomplished by synchronizing the generator with offsite power. The loading and unloading of an emergency diesel generator during this test should be gradual and based on a prescribed schedule that is selected to minimize stress and wear on the diesel generator.

2.2.3 Fast-Start Test: Demonstrate that each emergency diesel generator unit starts from standby conditions. If a plant normally has in operation pre-warm systems designed to maintain lube oil and jacket water cooling at certain temperatures or pre-lubrication systems or both, this would constitute normal standby conditions for that plant. Verify that the emergency diesel generator reaches required voltage and frequency within acceptable limits and time as defined in the plant technical specifications.

2.2.4 Loss-of-Offsite-Power (LOOP) Test: Demonstrate by simulating a loss-of-offsite power that (1) the emergency buses are deenergized and the loads are shed from the emergency buses, and (2) the emergency diesel generator starts on the autostart signal from its standby conditions, attains the required voltage and frequency and energizes permanently connected loads within acceptable limits and time, energizes the autoconnected shutdown loads through the load sequencer, and operates for greater than or equal to 5 minutes.

2.2.5 SIAS Test: Demonstrate that, on a safety injection actuation signal (SIAS), the emergency diesel generator starts on the autostart signal from its standby conditions, attains the required voltage and frequency within acceptable limits and time, and operates on standby for greater than or equal to 5 minutes.

2.2.6 Combined SIAS and LOOP Tests: Demonstrate that the emergency diesel generator can satisfactorily respond to a LOOP in conjunction with SIAS in whatever sequence they might occur (e.g., loss-of-coolant accident (LOCA) followed by delayed LOOP or LOOP followed by LOCA). A simultaneous LOOP/LOCA event would be demonstrated by simulating a LOOP and SIAS and verifying that (1) the emergency buses are deenergized and loads are shed from the emergency buses, and (2) the emergency diesel generator starts on the autostart signal from its standby conditions, attains the required voltage and frequency and energizes permanently connected loads within acceptable limits and time, energizes autoconnected loads through the load sequencer, and operates for greater than or equal to 5 minutes.

2.2.7 Single-Load Rejection Test: Demonstrate the emergency diesel generator's capability to reject a loss of the largest single load while operating at power factor between 0.8 and 0.9 and verify that the voltage and frequency requirements are met and that the unit will not trip on overspeed.

2.2.8 Full-Load Rejection Test: Demonstrate the emergency diesel generator's capability to reject a load equal to 90 to 100 percent of its continuous rating while operating at power factor between 0.8 and 0.9, and verify that the voltage requirements are met and that the emergency diesel generator will not trip on overspeed.

2.2.9 Endurance and Margin Test: Demonstrate full-load carrying capability at a power factor between 0.3 and 0.9 for an interval of not less than 24 hours, of which 2 hours are at a load equal to 105 to 110 percent of the continuous rating of the emergency diesel generator, and 22 hours are at a load equal to 90 to 100 percent of its continuous rating. Verify that voltage and frequency requirements are maintained.

2.2.10 Hot Restart Test: Demonstrate hot refunctional capability at full-load temperature conditions (after it has operated for 2 hours at full load) by verifying that the emergency diesel generator starts on a manual or autostarts signal, attains the required voltage and frequency within acceptable limits and time, and operates for longer than 5 minutes. This test may be performed following the endurance and margin test above.

2.2.11 Synchronizing Test: Demonstrate the ability to (1) synchronize the emergency diesel generator with offsite power while the unit is connected to the emergency load, (2) transfer this load to the offsite power, and (3) restore the emergency diesel generator to ready-to-load status.

2.2.12 Protective Trip Bypass Test: Demonstrate that all automatic emergency diesel generator trips (except engine overspeed, generator differential, and those retained with coincident logic) are automatically bypassed upon an SIAS. This test may be performed in conjunction with Regulatory Positions 2.2.5 and 2.2.6.

2.2.13 Test Mode Change-Over Test: Demonstrate that with the emergency diesel generator operating in a test mode while connected to its bus, a simulated safety injection signal overrides the test mode by (1) returning the emergency diesel generator to standby operation and (2) automatically energizing the emergency loads from offsite power.

2.2.14 Redundant Unit Test: Demonstrate that, by starting and running both redundant units simultaneously, potential common failure modes that may be undetected in single emergency diesel generator unit tests do not occur.

2.3 Preoperational and Surveillance Testing

Table 1 relates preoperational and surveillance tests to the anticipated schedule for performance (e.g., preoperational, monthly surveillance, 6-month testing, scheduled refueling period, and 10-year testing).

All planned tests described in Regulatory Position 2.2 should be preceded by a prelube period and should be in general accordance with the manufacture's recommendations for reducing engine wear, including cool-down operation at reduced power followed by postoperation lubrication.

2.3.1 Preoperational Testing: A preoperational test program should be implemented for all emergency diesel generator systems following assembly and installation at the site. This program should include the tests identified in Table 1.

In addition, through a minimum of 25 valid start-and-load demands in accordance with Regulatory Positions 2.2.2 and 2.2.3 without failure on each installed emergency diesel generator unit, demonstrate that an acceptance level of reliability has been achieved to place the new emergency diesel generator into an operational category.

2.3.2 Surveillance Testing: After plants are licensed (after fuel load), periodic surveillance testing of each emergency diesel generator must demonstrate continued capability and reliability of the diesel generator unit to perform its intended function. When the emergency diesel generator is declared operational in accordance with plant technical specifications, the following periodic test program should be implemented.

2.3.2.1 Monthly Testing: After completion of the emergency diesel generator unit reliability demonstration during normal plant operation should be performed. Each diesel generator should be started as described in Regulatory Position 2.2.1 and loaded as described in Regulatory Position 2.2.2 at least once in 31 days (with maximum allowable extension not to exceed 25 percent of the surveillance interval).

2.3.2.2 Six-Month (or 184 days) Testing: (This test may be substituted for a monthly test.) In order to demonstrate the capability of the emergency diesel generator to start from standby and provide the necessary power to mitigate the loss-of-coolant accident coincident with the loss of offsite power, once every 6 months each diesel generator should be started from standby conditions as described in Regulatory Position 2.2.3 to verify that the diesel generator reaches required voltage and frequency within acceptable limits and time as specified in the plant technical specifications. Following this test, the emergency diesel generator should be loaded as described in Regulatory Position 2.2.2 (See also Table 1.)

2.3.2.3 Refueling Outage Testing: Overall emergency diesel generator unit design capability should be demonstrated at every refueling outage by performing the tests identified in Table 1.

2.3.2.4 Ten-Year Testing: Demonstrate that the trains of standby electric power are independent once every 10 years (during a plant shutdown) or after any modifications that could affect emergency diesel generator independence, whichever is the shorter, by starting all redundant units simultaneously to help identify certain common failure modes undetected in single diesel generator unit tests. (See also Table 1.)

Table 1 of the Regulatory Guide is essentially the same as Table 3 of IEEE Std 387-1995. These tables show types of tests that must be done and at what stage the test is performed. The standard lists "site" tests and "pre-operational" tests that in total are equivalent to the pre-operational tests listed in the Regulatory Guide. It should be noted that SIAS and combined SIAS and LOOP tests are not applicable to the MFFF, as there is no equivalent safety injection signal at this facility. The descriptions of the tests in the two documents are also essentially equivalent. DCS will fully test the emergency diesel generators in accordance with the requirements of the standard.

Action:

None

157. Section 11.5.7.1, p. 11.5-14

Discuss any significant difference (applicable to MOX) between IEEE Standard 308-1991, "IEEE Standard Criteria for Class 1E Power Systems for Nuclear Generating Stations," and the 1974 version of this standard. Discuss how the DCS commitment to IEEE Standard 308-1991 meets the guidance provided in Regulatory Guide 1.32, "Criteria for Safety-Related Electric Power Systems for Nuclear Power Plants."

DCS has committed to IEEE Standard 308-1991. The NRC staff, in Regulatory Guide 1.32, has endorsed the 1974 version of this standard.

Per Section 11.3 of the SRP, information is recommended to determine if the design basis adequately addresses the functional requirements for the system. Per Section 11.4.2.2 of the SRP, electrical systems should be available and reliable and designed with specific considerations such as those contained in IEEE Standard 308 and Regulatory Guide 1.32.

Response:

IEEE Std 308 has been revised several times since the 1974 version was issued. In 1978, the standard was revised to clarify the interface between the functional requirements of the Class 1E power system and the safety systems for elements of the safety system that are within the Class 1E power system. The 1980 version of the standard implemented the recommendations of the Ad Hoc IEEE Std 308/603 Committee regarding the scope diagram for the IEEE Std 308 and Std 603 interface. IEEE Std 308-1991 is a general revision to the previous standard. The standard has been expanded to include the criteria for interfacing the Class 1E power system with IEEE Std 765-1983, "IEEE Standard for the Preferred Power Supply for Nuclear Power Generating Stations," and with IEEE Std 741-1990, "IEEE Standard Criteria for the Protection of Class 1E Power Systems and Equipment in Nuclear Power Generating Stations." The standard was also updated to reflect the requirements of IEEE Std 387-1984, "IEEE Standard Criteria for Diesel Generator Units Applied as Standby Power Supplies for Nuclear Power Generating Stations;" IEEE Std 946-1985, "IEEE Recommended Practice for the Design of Safety Related DC Auxiliary Power Systems for Nuclear Power Generating Stations;" and the recommendations of the NPEC Ad Hoc Committee on Shared Safety Systems. These recommendations resulted in a complete rewrite of Section 8, Multiunit Station Considerations, which obviously does not apply to the MFFF. It should be noted that when IEEE Std 308 refers to standby power systems, it is equivalent to MFFF emergency power systems. MFFF also has a "standby" power system but it is non-IROFS.

The following are statements of the positions of Regulatory Guide 1.32 and the sections from the 1991 revision of the standard that address the Regulatory Guide concerns.

Regulatory Guide 1.32, revision 2, February 1977, found the 1974 version of the standard generally acceptable subject to the following:

1 (a) Availability of Offsite Power. Consistent with the requirements of Criterion 17, the phrase "within an acceptable time" in Section 5.2.3 (4), first paragraph, of IEEE Std 308-1974 should be

construed to mean "within a few seconds". A preferred design would include two immediate access circuits from the transmission network. Detailed guidance for operating procedures and restrictions are acceptable to the staff, applicable where two immediate access circuits are available, is contained in Regulatory Guide 1.93, "Availability of Electric Power Sources". An acceptable design would substitute a delayed access circuit for one of the immediate access circuits provided the availability delayed of the access circuit conforms to Criterion 17.

Section 6.2.3, Preferred Power Supply, of the 1991 standard does not use the wording cited above but refers the user to IEEE Std 765-1983 for preferred power supply requirements. Section 4.5 (d), Availability, of IEEE Std 765-1995 states, " A minimum of one PPS circuit shall be designed to be available automatically to provide power to the Class 1E buses within a few seconds following a design basis accident. A second PPS circuit shall be designed to be available within a time period demonstrated to be adequate by the safety analysis of the station". The concern listed in the Regulatory Guide has been addressed in the standard. It should be noted, however, that the design of the MFFF, since it is not a nuclear power generating station, calls for the normal plant supply to be provided from two offsite sources. These sources supply the IROFS electrical equipment in the normal configuration. Also, unlike a generating station, loss of station service is not a consequence of an internal event in the MFFF. The offsite power source is the normal power source.

1 (b) Battery Charger Supply. The provisions of Section 5.3.4 of IEEE Std 308-1974 should be construed to mean that the capacity of the battery charger supply should be based on the largest combined demands of the various steady-state loads and the charging capacity to restore the battery from the design minimum charge state to the fully charged state, irrespective of the status of the plant when the demands occur.

Section 6.3.4 (3) of the 1991 standard addresses this issue with the following wording, "The capacity of each battery charger shall be based on the largest combined demands of the various continuous steady-state loads plus charging capacity to restore the battery from the design minimum charge state to the fully charged state within the time stated in the design basis regardless of the status of the plant during which these demands occur."

1 (c) Battery Performance Discharge Tests. The test interval for the battery performance discharge test should be as specified in IEEE Std 450-1975 instead of the 3 years specified in Table 2, "Illustrative Periodic Tests", of IEEE Std 308-1974. The battery service test described in IEEE Std 450-1975 should be performed in addition to the battery performance discharge test. The battery service test should be performed during refueling operations or at some other outage, with intervals between tests not to exceed 18 months. The note following Table 2 of IEEE Std 308-1974 should reference IEEE Std 450-1975 rather than IEEE Std 450-1972.

Section 7.4.2 of IEEE Std 308-1991 requires that tests be performed at scheduled intervals in accordance with IEEE Std 338-1987. Section 6.5 of IEEE Std 338 addresses the factors that should be considered when establishing initial test intervals and changes to those intervals.

1 (d) Independence of Redundant Standby Sources. Electrical independence between redundant standby (onsite) power sources should be in accordance with Regulatory Guide 1.6. Physical independence should be in accordance with Regulatory Guide 1.75. See response to Question 161 for

MFFF position on Regulatory Guide 1.75. Regulatory Guide 1.6 takes 5 regulatory positions as follows:

1) The electrically powered safety loads (a-c and d-c) should be separated into redundant load groups such that loss of any one load group will not prevent the minimum safety functions from being performed.

This is consistent with the MFFF design philosophy.

2) Each a-c load group should have a connection to the preferred (offsite) power source and to a standby (onsite) power source (usually a single diesel generator). The standby power source should have no automatic connection to any other redundant load group. At multiple nuclear unit sites, the standby source for one load group may have an automatic connection to a load group of a different unit. A preferred power source bus, however, may serve redundant load groups.

Each a-c load group at the MFFF has a connection to the preferred (offsite) power source and to an emergency diesel generator (onsite).

3) Each d-c load group should be energized by a battery and battery charger. The battery-charger combination should have no automatic connection to any other redundant d-c load group.

This is consistent with the MFFF design philosophy.

4) When operating from the standby sources, redundant load groups and the redundant standby sources should be independent of each other at least to the following extent:

(a) The standby source of one load group should not be automatically paralleled with the standby source of another load group under accident conditions;

(b) No provisions should exist for automatically connecting one load group to another load group;

(c) No provisions should exist for automatically transferring loads between redundant power sources;

(d) If means exist for manually connecting redundant load groups together, at least one interlock should be provided to prevent an operator error that would parallel their standby power sources.

These requirements are consistent with the MFFF design although MFFF has no provisions for paralleling redundant load groups.

5) A single generator driven by a single prime mover is acceptable as the standby power source for each a-c load group of the size and characteristics typical of recent applications. If other arrangements such as multiple diesel generators operated in parallel or multiple prime movers driving a single generator are proposed, the applicant should demonstrate that the proposed arrangement has an equivalent reliability. Common mode failures as well as random single failures should be considered in the analysis.

Standby diesel generators with a single prime mover driving a single generator will be used at the MFFF.

1 (e) Connection of Non-Class 1E Equipment to Class 1E Systems. The guidance presented in Regulatory Guide 1.75 should be followed.

See the response to Question 161 for the DCS physical independence position.

1(f) Selection of Diesel Generator Set Capacity for Standby Power Supplies. The guidance presented in Regulatory Guide 1.9 should be followed.

See the response to Question 156 for the DCS position on standby diesel generator set application.

2 (a) Shared Electric Systems for Multi-Unit Nuclear Power Plants. The provisions of Section 8.2 of IEEE Std 308-1974, which permit sharing of standby power supplies among units of a multi-unit station, are unacceptable except as specified in Regulatory Guide 1.81. The provisions of Section 8.3.1 of IEEE Std 308-1974 that permit sharing of battery supplies among units at a multi-unit plant are considered unacceptable and should be supplanted by the recommendations of Regulatory Guide 1.81.

This subject is not applicable to the MFFF; however, the 1991 version of the standard has entirely rewritten Section 8 of the standard dealing with this topic.

2 (b) Availability of Electric Power Sources. Table 3, "Suggested Operating Alternatives with Degraded Class 1E Power System Conditions" of IEEE Std 308-1974 is considered unacceptable and should be supplanted by the recommendations of Regulatory Guide 1.93.

The 1991 version of the standard does not contain the section described above.

Based on the above, DCS believes commitment to IEEE Std 308 1991 meets or exceeds guidance in Regulatory Guide 1.32.

Action:

None

158. Section 11.5.7.1, p. 11.5-14

Discuss any significant difference (applicable to MOX) between IEEE Standard 323-1983, "IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations," and the 1974 version of this standard.

DCS has committed to IEEE Standard 323-1983. The NRC staff, in Chapter 7 of NUREG-0800, has endorsed the 1974 version of this standard.

Per Section 11.3 of the SRP, information is recommended to determine if the design basis adequately addresses the functional requirements for the system. Per Section 11.4.2.2 of the SRP, electrical systems should be available and reliable and designed with specific considerations such as those contained in IEEE Standard 323.

Response:

IEEE Std 323-1983, *IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations*, was revised to clarify requirements and update references as applicable. The principal differences between the 1983 version of the standard and the 1974 version are the following:

- The definitions have been revised to eliminate some of the more obvious items (e.g., containment, demonstration, nuclear generating station, etc.) in favor of more subject specific terms (e.g., mild environment, harsh environment, aging, qualification, etc.).
- The On-Going Qualification section is not contained in the 1983 standard.
- The new standard adds provisions for control of modifications during tests as a requirement of the test plan for type testing.
- The suggested general categories for measured variables in test sequences are not contained in the 1983 version of the standard.
- The 1983 standard clarifies that for environmental transients two methods that may be used to apply margin are: (1) temperature and pressure margin may be added or (2) the peak transient without temperature and pressure margin may be applied twice. The standard also clarifies that the margin factors listed in the standard are not to be applied to aging.
- The 1983 standard provides guidance for when radiation testing may be excluded.
- The 1983 standard expands on extrapolation and interpolation by providing criteria that must be met if similarity is to be used.
- The 1983 standard provides a section that addresses extension of qualified life. This section provides methods that may be used to extend qualified life.
- There are no Appendices in the 1983 version of the standard.

The differences listed above provide clarifications and more updated information of equipment qualification programs and documentation. The changes do not add or delete any requirements from qualification programs. There are no significant changes that would affect or be applicable to the MFFF.

Action:

None

159. <u>Section 11.5.7.1, p. 11.5-14</u>

Discuss any significant difference (applicable to MOX) between IEEE Standard 344-1987, "IEEE Recommended Practices for Seismic Qualification of Class 1E Equipment for Nuclear Generating Stations," and the 1975 version of this standard. Discuss how the DCS commitment to IEEE Standard 344-1987 meets the guidance provided in Regulatory Guide 1.100, "Seismic Qualification of Electric Equipment for Nuclear Power Plants."

DCS has committed to IEEE Standard 344-1987. The NRC staff, in Regulatory Guide 1.100, has endorsed the 1975 version of this standard.

Per Section 11.3 of the SRP, information is recommended to determine if the design basis adequately addresses the functional requirements for the system. Per Section 11.4.2.2 of the SRP, electrical systems should be available and reliable and designed with specific considerations such as those contained in IEEE Standard 344 and Regulatory Guide 1.100.

Response:

Regulatory Guide 1.100, Revision 1, dated 8/77, endorsed IEEE Std 344-1975 subject to four exceptions. The current version of this standard is IEEE Std 344-1987. IEEE Std 344-1987 satisfactorily resolved those exceptions. Regulatory Guide 1.100, Revision 2, dated 6/88, reflects the resolution of the exceptions and accepts the 1987 version of the standard subject to the following:

> For mechanical equipment, thermal distortion effects on operability should be considered, and all loads on imposed on attached piping should be accounted for
>
> If dynamic testing of a pump or a valve assembly is impracticable, static testing of the assembly is acceptable provided that (1) the end loadings are applied and are equal to or greater than postulated event loads, (2) all dynamic amplification effects are accounted for, (3) the component is in the operating mode during and after the application of loads, (4) an adequate analysis is made to show the validity of the static application of loads.

This position is not applicable to electrical equipment and has no impact on the qualification of MFFF electrical equipment to the requirements of IEEE Std 344-1987, and therefore meets the guidance of Regulatory Guide 1.100.

Action:

None

160. Section 11.5.7.1, p. 11.5-14

Discuss any significant difference (applicable to MOX) between IEEE Standard 379-1994, "IEEE Standard Application of the Single Failure Criterion to Nuclear Power Generating Station Safety Systems," and the 1988 version of this standard.

DCS has committed to IEEE Standard 379-1994. The NRC staff, in Chapter 7 of NUREG-0800, has endorsed the 1988 version of this standard.

Per Section 11.3 of the SRP, information is recommended to determine if the design basis adequately addresses the functional requirements for the system. Per Section 11.4.2.2 of the SRP, electrical systems should be available and reliable and designed with specific considerations such as those contained in IEEE Standard 379.

Response:

IEEE Std 379-1994 was revised to:

- Clarify that safety systems shall be capable of performing their safety functions with the single failure occurring prior to or during the design basis event
- Revise the definitions to agree with IEEE Std 603-1991
- Update references cited in the text.

There are no substantive differences between the 1988 revision and the 1994 revision of IEEE Std 379. Several paragraphs from the 1988 standard are now individual sections (see Sections 6.2.6, 6.3.1, 6.3.2, and 6.3.3 of the 1994 standard), but nothing of significance has changed in the requirements of the document.

Action:

None

161. <u>Sections 11.5.7.1 and 11.5.7.2, p. 11.5-14 and 11.5-15</u>

Provide discussion/justification for deviations (applicable to MOX) from the minimum separation distances specified in Regulatory Guide 1.75, "Physical Independence of Electric Systems."

The NRC staff; in Regulatory Guide 1.75 endorses (with exceptions) IEEE Standard 384-1974, "Standard Criteria for Independence of Class 1E Equipment and Circuits." DCS has committed to IEEE Standard 384-1992.

Per Section 11.3 of the SRP, information is recommended to determine if the design basis adequately addresses the functional requirements for the system. Per Section 11.4.2.2 of the SRP, electrical systems should be available and reliable and designed with specific considerations such as those contained in IEEE Standard 384 and RG 1.75.

Response:

DCS has committed to follow the guidance of IEEE Std 384-1992 because it provides more specific guidance for various raceway configurations than the 1974 version of the standard and the distances for separation are based on actual testing of the configuration where distances differ from the 1974 version. Where testing of the actual configuration was not done or was inconclusive, no changes from the 1974 standard separation distances were made. The 1974 version of the standard recognizes two areas: cable spreading areas and general plant areas. The 1992 version classifies areas based on the potential hazards in the area into one of three categories: non-hazard, limited-hazard, and hazard areas. Separation distances are then applied based on the area classification. Application of the hazard area definition of IEEE Std 384-1992 provides more realistic criteria to be applied to an industrial facility such as the MFFF where hazards such as HELB, jet impingement, internal missile, etc. do not exist.

The 1974 version of the standard is based on open ventilated cable trays of either the ladder or trough type. The 1992 version of the standard recognizes various raceway configurations and provides guidance under these conditions. The table below shows a comparison of the configurations addressed and the separation distances allowed.

CONFIGURATION	IEEE Std 384-1974	IEEE Std 384-1992
Non-Hazard Area		
Open Trays		1' hor ; 3' vert
Enclosed to Open		1" hor ; 3" vert
Enclosed Raceway		1" hor ; 1" vert
Limited Hazard Area		
Open Trays (2/0 & up and all Medium Voltage)		3' hor ; 5' vert
Open Trays (less than 2/0)		6" hor ; 12" vert
Open Trays (I&C)		1" hor ; 3" vert

CONFIGURATION	**IEEE Std 384-1974**	**IEEE Std 384-1992**
Enclosed to Open (2/0 & up and all Medium Voltage)		3' hor ; 5' vert
Enclosed to Open (less than 2/0)		6" hor ; 12" vert
Enclosed to Open (I&C)		1" hor ; 3" vert
Enclosed Raceway		1" hor ; 1" vert
Hazard Area		
	Only one division allowed in area	Only one division allowed in area
Internal Panel	6"	1" hor ; 6" vert
Cable Spreading Area		
Open to Open	1' hor ; 3' vert	
Enclosed Raceway	1" hor ; 1" vert	
General Plant Areas		
Open to Open	3' hor ; 5' vert	
Enclosed Raceway	1" hor ; 1" vert	

Section 5.1.1.2 of the 1974 version of the standard allows for minimum separation distances that are established by testing and analysis. The basis for the 1992 version of the standard was actual testing as documented in paper 90 WM 254-3 EC, *Cable Separation – What Do Industry Testing Programs Show?* The changes implemented in the 1992 version of the standard are in keeping with the spirit and direction of the 1974 version.

The NRC staff has endorsed the 1974 version of the standard with exceptions as noted in the 16 regulatory positions of the Regulatory Guide 1.75. The 1992 revision of IEEE Std 384 addresses the concerns raised by the Regulatory Guide exceptions. The following is a summary of the Commission's exceptions and the requirements in the 1992 revision of the standard that specifically address the exceptions.

Regulatory Position 1 asks for a supplement to the definition of Isolating Device that reads "Interrupting devices actuated only by fault current are not considered to be isolation devices within the context of this document". In the basis for this position, it is recognized that proper breaker or fuse coordination would preclude an upstream main circuit breaker from tripping because of conditions in another part of the circuit.

The 1992 version of the standard addresses this issue in Section 7. Where circuit breakers tripped by fault current are used for isolation, they can be considered isolation devices if the following criteria are met:

1) The breaker time-overcurrent characteristic for all circuit faults will cause the breaker to interrupt the fault current prior to initiation of a trip of any upstream breaker. Periodic testing shall demonstrate that the overall coordination scheme remains within the limits specified in the design criteria. The testing may be performed as a series of overlapping tests.

2) The power source shall supply the necessary fault current for sufficient time to ensure the proper coordination without loss of function of Class 1E loads.

Fuses may be used as a power isolation device if the following criteria are met:

1) Fuses shall provide the design overcurrent protection capability for the life of the fuse.

2) The fuse time-overcurrent trip characteristic for all circuit faults shall cause the fuse to open prior to the initiation of an opening of any upstream interrupting device.

3) The power source shall supply the necessary fault current to ensure the proper coordination without loss of function of Class 1E loads.

DCS will follow the requirements of Section 7 of the 1992 version of the standard with respect to proper coordination of protective devices and periodic testing to ensure coordination is maintained.

<u>Regulatory Position 2</u> states that interlocking armor cable should not be construed as a "raceway".

As noted in the basis for this position, this is not consistent with industry practice or the National Electric Code. DCS has no intentions of classifying interlocking armor cable as raceway. This issue is not specifically addressed in either the 1974 or 1992 versions of the standard.

<u>Regulatory Position 3</u> asks that Section 4.3 of the 1974 standard be supplemented as follows: "In general, locating redundant circuits and equipment in separate safety class structures affords a greater degree of assurance that a single event will not effect the redundant systems. This method of separation should be used whenever practicable and where its use does not conflict with other safety objectives".

This is a clarification and nothing in the 1992 version of the standard conflicts with this philosophy. This is the approach being used by DCS. The key word is "practicable". Location of IROFS electrical equipment has been in separate safety class structures; however, the routing of raceway will require that the separation distances and/or barriers be used in accordance with IEEE Std 384 due to physical limitations.

<u>Regulatory Position 4</u> states that "Associated circuits installed in accordance with Section 4.5(1) should be subject to all requirements placed on Class 1E circuits such as cable derating, environmental qualification, flame retardance, splicing restriction, and raceway fill unless it can be demonstrated that the absence of such requirements could not significantly reduce the availability of the Class 1E circuits".

Section 5.5.2 of the 1992 version of the standard has the following criteria for associated circuits. "Associated circuits shall comply with one of the following requirements:

1) They shall be uniquely identified as such or as Class 1E and shall remain with (traceable to the associated Class 1E division), or be physically separated the same as, those Class 1E circuits with which they are associated. They shall be subject to the requirements placed on Class 1E circuits, unless it can be demonstrated by analysis or testing that the absence of such requirements cannot degrade the Class 1E circuits below an acceptable level.

2) They shall be in accordance with 1) above from the Class 1E equipment to and including an isolation device. Beyond the isolation device, such a circuit is non-Class 1E provided that it does not again become associated with another Class 1E system.

3) They shall be analyzed or tested to demonstrate that Class 1E circuits are not degraded below an acceptable level.

The 1992 version of the standard meets the intent of the position by requiring that associated circuits be subject to the same requirements as the Class 1E circuits they are associated with, up to and including the isolation device; or an analysis or test be performed to demonstrate that the absence of such requirements cannot degrade the Class 1E circuits below an acceptable level.

Regulatory Position 5 asks that the note following Section 4.5 be supplemented with "This exemption is limited and does not extend to other requirements such as those of General Design Criterion 17."

The same note appears after Section 5.5.2 of the 1992 standard. DCS understands the limited nature of the exemption in the note. The use of the 1992 standard instead of the 1974 standard will not affect the approach DCS will take to applying the note referred.

Regulatory Position 6 asks that analyses performed in accordance with Sections 4.5 (3), 4.6.2, and 5.1.1.2 should be submitted as part of the Safety Analysis Report and should identify those circuits installed in accordance with these sections.

Separation distances provided in the 1992 revision of IEEE Std 384 are based on industry test data that have been reviewed by the IEEE Working Group and the specified distances are the conclusions of the working group's review. DCS is committing to the 1992 revision of the standard and will justify separation distances less than those used in the 1992 version of the standard. It is not anticipated that exceptions will be taken to the separation distances in the 1992 standard. An Independence Review will be performed at the conclusion of the construction phase to verify that separation criteria have not been violated.

Regulatory Position 7 states that non-Class 1E instrumentation and control circuits should not be exempted from the provisions of Section 4.6.2.

Section 4.6.2 of the 1974 standard addresses separation from associated circuits and allows the exemption stated above. The 1992 version of the standard qualifies this exemption if certain conditions are met in Section 5.6 (4):

> "Non-Class 1E instrumentation signal and control circuits (see IEEE Std 690-1984 [14]) are not required to be physically separated or electrically isolated from associated circuits provided that (a) the non-Class 1E circuits are not routed with associated cables of a redundant division and (b) the non-Class 1E circuits are analyzed to demonstrate that Class 1E circuits are not degraded below an acceptable level. As part of the analysis, consideration shall be given to potential energy and identification of the circuits involved".

These conditions prevent one non-Class1E circuit from damaging two Class 1E divisions and ensure that the non-Class 1E circuit will not degrade the Class 1E circuit.

<u>Regulatory Position 8</u> Section 5.1.1.1 should not be construed to imply that adequate separation of redundant circuits can be achieved within a confined space such as a cable tunnel that is effectively unventilated.

The 1992 standard has addressed this concern by adding some clarifying language to Section 6.1.1.1, Classification of Areas:

> "Separation commensurate with the damage potential of the hazard shall be provided for early in the design through the use of features such as separate rooms. Opposite sides of rooms or areas may be used provided that there is an adequate heat removal capability".

<u>Regulatory Position 9</u> asks that Section 5.1.1.3 be supplemented by adding "(4) Cable splices in raceways should be prohibited".

DCS will not allow splices to be made up in raceway. Boxes will be used if splicing is necessary.

<u>Regulatory Position 10</u> adds that in Section 5.1.2, the phrase "at a sufficient number of points" should be understood to mean at intervals not to exceed 5 feet throughout the entire cable length. Also, the preferred method of marking cable is color coding.

Section 6.1.2 of the 1992 standard has been modified to address this concern by adding the following wording: "... Cables installed in these raceways shall be marked in a manner of sufficient durability and intervals of approximately 5 ft. (1.5 m) to facilitate initial verification that the installation is in conformance with the separation criteria...."

<u>Regulatory Position 11</u> states that Section 5.1.2 should be supplemented as follows: "The method of identification should be simple and should preclude the need to consult any reference material to distinguish between Class 1E and non-Class 1E circuits, between non-Class 1E circuits associated with different Class 1E systems, and between redundant Class 1E systems".

Section 6.1.2 of the 1992 standard has been modified to address this concern by adding the following wording: ".... The method of identification used to meet the above requirements shall

readily distinguish between redundant Class 1E systems, between Class 1E and non-Class 1E systems and between associated cables of different redundant Class 1E systems".

The DCS cable and raceway identifiers provide for color coding and unique characters to identify Class 1E, non-Class 1E, and associated circuits.

Regulatory Position 12 states that pending issuance of other acceptable criteria, those portions of Section 5.1.3 (exclusive of the Note following the second paragraph) that permit the routing of power cables through the cable spreading area (s) and, by implication, the control room, should not be construed as acceptable. Also, Section 5.1.3 should be supplemented as follows: "Where feasible, redundant cable spreading areas should be utilized".

The 1992 standard addresses this issue with the definition and restrictions placed on non-hazard areas. Section 6.1.3.1, Area Designation, sets forth the following requirements for non-hazard areas that encompass control rooms and cable spreading areas from the 1974 standard:

1) The area shall not contain high energy equipment such as switchgear, transformers, rotating equipment, or potential sources of missiles or pipe failure hazards, or fire hazards.

2) Circuits in the area shall be limited to control and instrument functions and those power supply circuit cables and equipment serving the equipment located in the area.

3) Power circuit cables in this area shall be installed in enclosed raceways.

4) Administrative control of operations and maintenance activities shall control and limit introduction of potential hazards into the area.

Regulatory Position 13 states that no significance should be attached to the different tray widths illustrated in figure 2.

The 1992 standard has slightly different figures; however, it is understood that the figures illustrate tray separation distances and that the tray widths shown are not significant.

Regulatory Position 14 asks that Section 5.2.1 should be supplemented as follows: "And should have independent air supplies."

DCS MFFF is using electric start generators for emergency power. The auxiliaries for each generator will be completely independent.

Regulatory Position 15 states that where ventilation is required, the separate safety class structures required by Section 5.3.1 should be served by independent ventilation systems.

Each emergency battery room for MFFF has an independent ventilation system.

Regulatory Position 16 asks that the first paragraph of Section 5.7 be augmented as follows: "The separation requirements of 5.6 apply to instrumentation cabinets."

This issue is addressed in the 1992 standard in Section 6.7. "Instruments requiring separation per Section 5 shall be located in separate cabinets or compartments of a cabinet complying with *the requirements of 6.6.*"

Action:

None

162. Section 11.5.7.2, p. 11.5-15

Discuss DCS's lack of commitment to IEEE Standard 484-1975, "IEEE Recommended Practice for Installation Design and Installation of Large Lead Storage Batteries for Generating Stations and Substations."

Per Section 11.3 of the SRP, information is recommended to determine if the design basis adequately addresses the functional requirements for the system. Per Section 11.4.2.2 of the SRP, electrical systems should be available and reliable and designed with specific considerations such as those contained in IEEE Standard 484.

Response:

IEEE Std 484-1996, "Recommended Practice for Installation Design and Installation of Vented Lead-Acid Batteries for Stationary Applications," provides good general installation design guidance. DCS will comply with the guidance of the standard in the design and installation of the facility batteries. The 1996 revision of the standard will be used, as it is the current revision of record. Where other standards are referenced, the latest versions of those standards will be used.

The significant differences between the two versions of the standard are that in the new standard, there is the following:

- Section 2 - The references have been reduced to IEEE Standards 100, 450, and 485.
- Section 3 - The definitions have been reduced to "vented battery" only.
- Section 4.1 – Class C fire extinguishers have been added as protective equipment.
- Section 4.2 – Additional precautions have been added to ensure that the battery area is ventilated during charging, avoid wearing metallic objects while working on the battery, avoid excessive tilting of cells and to neutralize static buildup by having personnel contact a grounded surface before working on the battery.
- Section 5.5 – Each battery should have instrumentation to measure current through the battery.
- Section 6.2.2 – Requires that any connection that has a resistance measurement more than 10% or $5\mu\Omega$, which ever is greater, over the average for each type of connection be remade and remeasured.
- Section 6.3.1 – Allows the measurement of temperature and specific gravity from every tenth cell instead of each cell.
- Section 6.3.2.1 – This section has been added to address optional measurements.

- Section 6.3.3 – This section has been added to address acceptance tests.
- Section 6.4 – Calls for connection to the DC system after completion of the items in the standard.
- Annex A has been added to provide examples of various connections and a recommended method for performing connection resistance readings.
- Annex B has been added to provide information on cell/unit internal impedance measurements.

The standard has been strengthened with more clarifications and updated information and practices.

Action:

None

163. Section 11.5.7.2, p. 11.5-15

Discuss DCS's choice of IEEE Standard 485-1992, "IEEE Recommended Practice for Sizing Lead-Acid Batteries for Stationary Applications," and discuss any significant difference (applicable to MOX) between this version and the 1997 version.

DCS has committed to IEEE Standard 485-1992. Staff review and participation in the standard's development indicate that IEEE Standard 485-1997 is much improved.

Per Section 11.3 of the SRP, information is recommended to determine if the design basis adequately addresses the functional requirements for the system. Per Section 11.4.2.2 of the SRP, electrical systems should be available and reliable and designed with specific considerations such as those contained in IEEE Standard 485.

Response:

DCS will use IEEE Std 485-1997.

Action:

In the next update to the CAR, indicate the adoption of IEEE Std 485-1997.

164. Sections 11.6.6 and 11.6.7, pp. 11.6-12 thru 11.6-14

Discuss specific design considerations used in the MOX facility to minimize the effects of smoke on digital instrumentation and control components.

Recently; in NUREG/CR-6597, "Results and Insights on the Impact of Smoke on Digital Instrumentation and Control," the NRC discussed the effects of smoke on digital, electronic components.

Per Section 11.3 of the SRP, information is recommended to determine if the design basis adequately addresses the functional requirements for the system. Per Section 11.4.3.2 of the SRP, instrumentation and control systems should be available and reliable and designed with specific considerations such as those contained in NUREG/CR-6597.

Response:

The significant findings of NUREG/CR-6597 are summarized in Section 5.1.2 of NUREG/CR-6597, Methods of Smoke Protection, and are given as: prevent fires, control the movement of smoke, protect electronics by physical methods, and locate components to minimize exposure to fire and smoke. In general, the design for MFFF follows these methods:

a) Fire prevention is an important design consideration of the MFFF. See Chapter 7 of the CAR for descriptions of fire protection measures.

b) Movement of smoke is controlled in the facility by fire barriers and ventilation exhaust. See Section 11.4.8 of the CAR. The MFFF is divided up into more than 300 individual fire areas. Dispersing the digital electronics within these areas reduces the potential of exposure to smoke.

c) The digital electronics are located in cabinets and panels, which reduces the potential exposure to smoke.

d) Digital Electronics are located in electronic rooms, which are separate fire areas away from the process. Electronic rooms themselves are located throughout the facility. Redundant digital control equipment will be located in separate fire areas.

Action:

None

165. Section 11.6.7, pp. 11.6-12 thru 11.6-14

Describe the method of data communications independence as related to isolation of the safety control circuits and other circuits.

Section 11.6.7 of the application states that the software programmable electronic systems used in safety control subsystems are designed using the methods and practices identified in IEEE 7-4.3.2 - 1993, "IEEE Standard for Digital Computers in Safety Systems of Nuclear Power Generating Stations." Section 5.6 of that standard entitled "Independence," states that data communications between safety channels or between safety and non-safety systems shall not inhibit the performance of the safety function.

Per SRP Section 11.4.3.2, information is recommended to determine if the design basis adequately addresses the maintenance of redundancy and independence. Data communications independence is a special case of independence for digital systems. The information submitted should include both the hardware and software basis of data communications independence.

Response:

The basis for independence of data communications between (digital) safety control circuits and non-safety circuits are provided in IEEE Std 603-98, IEEE Std 7.4.3.2-1993, and IEEE Std 384-92. IEEE Std 603 criteria requires that the digital safety controls shall be designed such that any credible failure of interconnected non-safety circuits shall not prevent the safety controller from meeting its performance requirements. IEEE Std 7.4.2.3 provides additional clarification of the requirements of IEEE Std 603 by explicitly requiring that data communications between safety and non-safety systems shall not inhibit the performance of the safety system. IEEE Std 384 provides the physical requirements for achieving independence by physical separation and electrical isolation.

The design for independence of data communications between safety and non-safety digital controllers will be in accordance with IEEE Std 7.4.3.2 section 5.6 and will use the techniques delineated in Appendix G of the same standard. The techniques described in Appendix G of IEEE Std 7.4.3.2 are also in accordance with the criteria of IEEE Std 603 and IEEE Std 384.

Action:

None

166. Section 11.6.7, pp. 11.6-12 thru 11.6-14

Describe the planned degree of conformance with the specific criteria of IEEE Standard 4-7.4.3.2-1993, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations," for the software programmable systems used in safety control subsystems.

In Section 11.6.7 of the application, the phrase "using the methods and practices" of the particular standard does not specifically identify the actual degree of conformance to the criteria of the standard.

Per Section 11.4.1, 11.5.1 of the SRP, information is recommended to determine if the design basis adequately addresses the specific criteria of the referenced standard in order to verify the applicant's commitment to provide plant systems that satisfy the acceptance criteria.

Response:

The following is a description of applicability of IEEE Std 7-4.3.2 requirements to the MFFF (a non-reactor facility)

IEEE Std 7-4.3.2 §1,2 &3

These sections do not provide design criteria.

IEEE Std 7-4.3.2 §4 Safety System Design Basis

DCS will conform to this section with the following clarifications:

- Application of IEEE Std 603 to the MFFF design basis will be in context of our response to Question 173.
- ANSI/ANS 51.1 and ANSI/ANS 51.2 are not applicable to a fuel facility. Consistency of design basis with these standards will not be addressed.

IEEE Std 7-4.3.2 §5 Safety System Criteria

DCS will conform to all parts of this section with the following amplifications:

- The referenced QA standard for software development is ASME NQA-2a, Part 2.7, which has been incorporated into ASME NQA-1-1994 (1995a Addenda). As the DCS QA Program is based on NQA-1, NQA-1 will be used for software development.
- Subsection 5.13 specifies requirements for Multi-unit (generating) stations and is not applicable to the MFFF Design.

IEEE Std 7-4.3.2 §6 Sense and Command Features

DCS will conform to this section with the application of IEEE Std 603 in the context of the response to Question 173.

IEEE Std 7-4.3.2 §7 Execute Features.

DCS will conform to this section with the application of IEEE Std 603 in the context of the response to Question 173.

IEEE Std 7-4.3.2 §8 Power Source Requirements

DCS will conform to this section with the application of IEEE Std 603 in the context of the response to Question 173.

IEEE Std 7-4.3.2 Annexes A-H

Annexes A-H are not part of the standard and are provided for information. DCS will use the Annexes for information.

Action:

Clarify IEEE Std 7-4.3.2 §§ 4 and 5 in the CAR.

167. Section 11.6.7, pp. 11.6-12 thru 11.6-14

Describe how the system hazards that the software components are expected to handle will be included in the requirements for the software components.

Software is frequently overlooked during system hazard analyses, but this should not occur in safety applications. Software hazard analysis controls software hazards and hazards related to interfaces between the software and the system (including hardware and human components.) It includes analyzing the requirements, design, implementation, user interfaces and changes. The description of methods, practices, or standards concerning the allocation of system hazards to software components and their inclusion in the requirements is missing in the application.

Per Section 11.3, 11.4.3.2, and 11.5.1 of the SRP, a determination should be made if the design basis adequately addresses the specific criteria of: (a) the assurance measures, including applicable codes and standards; and (b) the provisions so that I&C components fail in a safe manner. Information is needed in order to evaluate the applicant's commitment to provide plant systems that satisfy the acceptance criteria.

Response:

System hazards are identified in the ISA; see Chapter 5 of the CAR. The results of the ISA will be incorporated into the control system technical descriptions, which are one of the requirement document types that input to the software development process. The control system descriptions are technical documents prepared and controlled under the DCS QA program. Control system descriptions for principal SSCs are quality level 1 documents requiring both review and design verification.

The performance requirements of the software will be specified and developed in accordance with the programmatic requirements identified in the software life cycle program. This program is currently under development. However, there are some fundamental bases for the software development of QL-1 systems that can be presented:

1. The software life cycle model will be developed in accordance with IEEE Std 1074-1997, "Standard for Developing Software Life Cycle Processes"

2. The software for any programmable electronic system will be assigned to the highest level of software integrity as identified in IEEE Std 1012-1998, Software Verification and Validation.

3. The software specifications will be produced in accordance with IEEE Std 830-1998, "IEEE Recommended Practice for Software Requirements Specifications"

4. A software safety plan will be developed for each digital controller that is an SSC. The software safety plan will be prepared in accordance with IEEE Std 1228 "Standard for Software Safety Plans".

Action:

None

168. Section 11.6.7, pp. 11.6-12 thru 11.6-14

Describe what methods, practices, or standard(s) that will be used for the software design documentation.

The description of methods, practices, or standards concerning the documentation of the software design is not described in the application. A consistent documentation method for the software is necessary for all the reviews, verification and validation, and other assurance measures.

Per Section 11.3 and 11.5.1 of the SRP, a determination should be made if the design basis adequately addresses the specific criteria of the assurance measures, including applicable codes and standards. Information is needed in order to evaluate the applicant's commitment to provide plant systems that satisfy the acceptance criteria.

Response:

At this stage in the design of the MFFF, the detailed descriptions of each software phase are in development and are not yet available. Documentation of the software at the various phases of its life cycle will be in accordance with the procedures and requirements that will be defined in the software configuration management process that is currently under development. The software documentation will be provided with the License Application.

The standards that will be used for the software development for digital controllers that are principal SSCs are:

1. Software Life Cycle process (IEEE Std 1074-1997)
2. Software V&V process (IEEE Std 1012-1998)
3. Software Configuration Management process (IEEE Std 828-1998 and IEEE Std 1042-1987)
4. Software Quality Assurance program (IEEE Std 730-1998)
5. NQA-1a-1995 Subpart 2.7

Action:

None

169. <u>Section 11.6.7, pp. 11.6-12 thru 11.6-14</u>

Describe the methods, practices or standard(s) under which previously developed software or purchased software involved in safety functions will be controlled, reviewed, verified and validated.

The assurance measures, including applicable codes and standards, for previously developed or purchased software that is used in safety functions is not described in this section of the application.

Per Section 11.3 and 11.5.1 of the SRP, a determination should be made if the design basis adequately addresses the specific criteria of the assurance measures, including applicable codes and standards. Information is needed in order to evaluate the applicant's commitment to provide plant systems that satisfy the acceptance criteria.

Response:

Software used in digital computer equipment that are principal SSCs will be controlled under the MOX Project Quality Assurance Plan (MPQAP); see Chapter 15 of the CAR. In particular, the MPQAP invokes ASME NQA-1a (1995) Subpart 2.7 requirements for computer software whether it is purchased, modified existing software, or newly developed software. The specific procedures that delineate the methods of that control software procurement or modification are under development at this time. These procedures are based on the IEEE standards for computer life cycle development that are listed in the response to Question 168.

Action:

None

170. Section 11.6.7, pp. 11.6-12 thru 11.6-14

Describe the methods, practices or standard(s) that will be used for the software programming language(s) involved in safety applications.

The assurance measures, including applicable codes and standards, for software programming languages that are planned to be used in safety functions is not described in this section of the application. The programming language can have effects on safety functions if certain features of the language are used. For information, the potential effects of programming languages are discussed in NUREG/ CR-6463, Revision 1, "Review Guidelines for Software Languages for Use in Nuclear Power Plant Safety Systems."

Per Section 11.3 and 11.5.1 of the SRP, a determination should be made if the design basis adequately addresses the specific criteria of the assurance measures, including applicable codes and standards. Information is needed in order to evaluate the applicant's commitment to provide plant systems that satisfy the acceptance criteria.

Response:

For programmable logic controllers used in IROFS applications, the languages used will be the industry accepted real time control languages specified in IEC 60113-3 (1993-03) Programmable controllers-Part 3: Programming Languages. The languages that are expected to be used for programmable controllers will be the Sequential Functional Chart (SFC) language or Ladder Logic language. For other applications, the software that DCS develops for IROFS will be written using the C language. These are addressed in NUREG/CR-6463 and are the languages used in the reference plants, MELOX and La Hague.

The rules for implementation of the software (the particular coding methods, practices and standards for each of the programming languages that might be used for programming safety applications) will be established as part of the software lifecycle program. The software lifecycle development is part of the detailed design phase of the project and will be described with the license application for possession and use of special nuclear material.

Action:

None

171. Section 11.6.7, pp. 11.6-12 thru 11.6-14

Describe the planned application of IEEE 1074-1997 to the life cycle processes of the application software for the digital computers used in safety systems.

The application states that the application software life cycle will be developed, reviewed, and verified using the methods and practices identified in IEEE 1074-1997, "IEEE Guide for Developing Software Life Cycle Processes." The correct title of IEEE 1074-1997 is "IEEE Standard for Developing Software Life Cycle Processes."

In Section 11.6.7 of the application the phrase "using the methods and practices" of the particular standard does not specifically identify the actual degree of conformance to the detailed criteria of the referenced standard.

Per Section 11.4.1 and 11.5.1 of the SRP, information is required to determine if the design basis adequately addresses the specific criteria of the referenced standards in order to evaluate the applicant's commitment to provide plant systems that satisfy the acceptance criteria.

Note: Acceptance for software based equipment is based on the SRP and additional guidance in NUREG-0800, Chapter 7 (Instrumentation & Controls) for digital systems, software, real-time performance, data communications, and programmable logic controllers. In general, acceptance is based on the adequate confidence that the allocation of system hazards to software, the functional behavior that the software is to exhibit as specified in the requirements, and the characteristics of the software development process for the particular software life cycle, will result in a system that will meet the recommendations of SRP Section 11.4.1.

Response:

The correct title of IEEE Std 1074 is as noted in the question. This will be corrected.

Software lifecycle models will be developed as necessary to accommodate software derived from legacy code and newly developed software. Software lifecycles will be developed in accordance with IEEE Std 1074-1997, IEEE Guide Standard for Developing Software Life Cycle Processes, recognizing the caveats identified in Regulatory Guide 1.173. DCS will commit to Regulatory Guide 1.173 except that DCS will use the 1997 issue of IEEE Std 1074, not the 1995 issue identified in Regulatory Guide 1.173. Refer to Question 178 for a discussion of the differences between the two issues of IEEE Std 1074.

Action:

Correct the title of IEEE Std 1074 and clarify the commitment to Regulatory Guide 1.173 in the next update of the CAR.

172. Section 11.6.7, p. 11.6-13

Clarify the degree of DCS's commitment to standards and codes.

Sections 11.4.1 and 11.5.1 of the SRP recommend that information be provided to determine if the design basis adequately addresses the specific criteria of the referenced standards in order to evaluate the applicant's commitment to provide plant systems that satisfy the acceptance criteria. The application states, "The following codes and standards, as applicable to fuel cycle facilities, are used in the design of I&C principal SSCs." This sentence does not provide a clear commitment to standard and codes. Also, the phrase, "using the methods and practices," does not specifically identify the actual degree of conformance to the detailed criteria of a referenced standard.

Response:

There are few industry consensus standards available for the development of electrical and instrument & control system designs used in a mixed oxide fuel fabrication facility. DCS has chosen to adopt standards that were written to provide criteria and requirements for safety systems in commercial nuclear power generating stations to provide a proven and accepted means for the design of safety systems. The caveat statements in the CAR ("...as applicable..." and "...using methods and practices...") were added to allow flexibility for requirements that obviously are not applicable to the fuel fabrication facility. As an example, IEEE Std 603 identifies reactor trips and emergency safety feature equipment as safety system equipment and the MFFF clearly does not have these types of components. However, the criteria that are provided for the design of safety systems will be used for the design of SSCs for the MFFF as they are directly applicable to any high consequence engineered system regardless of the industry. DCS commits to applying the requirements of codes and standards identified in the CAR except for requirements that obviously apply to SSCs unique to a nuclear reactor. These points are further elaborated in the responses to the questions that directly address concerns with particular standards.

Action:

None

173. Section 11.6.7, p. 11.6-13

Discuss any significant difference (applicable to MOX) between IEEE Standard 603-1998, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," and the 1991 version of this standard. Discuss how the DCS commitment to IEEE Standard 603-1998 meets the guidance provided in Regulatory Guide 1.153, "Criteria for Safety Systems."

DCS has committed to IEEE Standard 603-1998. The NRC staff, in Regulatory Guide 1.153, has endorsed the 1991 version of this standard.

Per Section 11.3 of the SRP, information is recommended to determine if the design basis adequately addresses the functional requirements for the system. Per Section 11.4.3.2 of the SRP, instrumentation and control systems should be available and reliable and designed with specific considerations such as those contained in IEEE Standard 603 and Regulatory Guide 1.153.

Response:

IEEE Std 603-1998 was revised to clarify the application of the standard to computer based safety systems and to advanced nuclear power generating station designs. The revision provides guidance for the treatment of electromagnetic interference (EMI) and radio frequency interference (RFI), clarifies definitions, and updates references.

The following are contained in the 1998 version of the standard that are not contained in the 1991 version:

- A definition is presented for common-cause failure in 3.10 of the standard.
- A note has been added to the definition of division (3.14) to clarify that a division can have one or more channels
- A note has been added to the definition of redundant equipment or system (3.22) to clarify that duplication of essential function can be accomplished by the use of identical equipment, equipment diversity or functional diversity.
- Electromagnetic Interference has been added to section 4 (g) as an example of on e of the conditions that must be documented in the design basis.
- IEEE Std 7-4.3.2-1993 has been added as a reference to provide guidance on the use of digital computers concerning single failure criterion (5.1), quality (5.3), equipment qualification (5.4), system integrity (5.5), detailed criteria (5.6.4), identification (5.11) and reliability (5.16).
- A clarification was added to section 5.1 to indicate that a single failure could occur prior to, or at any time during, the design basis event for which the safety system is required to function.
- Section 5.16, Common Cause Failure Criteria, has been added.

- Section 6.5.2 (b), "the period of time it" has been added before the word retains. This requires that the period of time the equipment that is identified as being stable post accident retains its calibration during the post accident time period be identified.
- Section 6.7, the word shall has been changed to should in the last sentence. "During such operation, the sense and command features should continue to meet the requirements of 5.1 and 6.3".
- Annex B has been added to provide information on Electromagnetic Compatibility. References are provided as well as coupling mechanisms that must be considered and typical protection techniques.

The significant enhancements to this standard are the acknowledgement that digital computer may be used in safety systems and the reference to the guidance of IEEE Std 7-4.3.2-1993, and the requirement to consider EMI in the design.

Regulatory Guide 1.153, Rev.1 states that IEEE Std 603-1991 provides a method acceptable to the NRC staff for satisfying the Commission's regulations with respect to the design, reliability, qualification, and testability of the power, instrumentation, and controls portions of the safety systems of nuclear power plants. Commitment to the 1998 version of the standard does not diminish position stated in Regulatory Guide. The later standard in fact enhances the requirements of the guide because it addresses safety systems using digital computers and addresses EMI in the design basis requirements.

Action:

None

174. Section 11.6.7, p. 11.6-13

Discuss any significant difference (applicable to MOX) between IEEE Standard 828-1998, "IEEE Standard for Software Configuration Management Plans," and the 1990 version of this standard. Discuss how the DCS commitment to IEEE Standard 828-1998 meets the guidance provided in Regulatory Guide 1.169, "Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants."

DCS has committed to IEEE Standard 828-1998." The NRC staff, in Regulatory Guide 1.169, has endorsed the 1990 version of this standard.

Per Section 11.3 of the SRP, information is recommended to determine if the design basis adequately addresses the functional requirements for the system. Per Section 11.4.3.2 of the SRP, instrumentation and control systems should be available and reliable and designed with specific considerations such as those contained in IEEE Standard 828 and Regulatory Guide 1.169.

Response:

The content of IEEE Std 828-1998 is essentially unchanged from IEEE Std 828-1990.

The technical requirements in clauses 4 through 6 (old sections 3 through 4) remain identical.

The differences are as follows:

- The paragraph structure has been re-numbered and references within the text have been changed to properly reflect the new numbering structure.
- The term "section" has been replaced with "clause" when referring to the parts of the standard.
- The second sentence of the second paragraph of Section 4.3.1 (old Section 2.3.1) has been changed to read "...the plan shall state..." from "...the plan states..."
- The third sentence of the second paragraph of Section 4.3.1 (old Section 2.3.1) has been changed to read "Information required for configuration identification (see figure 1) is specified in 4.3.1.1 through 4.3.1.3." from "The following sections specify information required for configuration identification (see figure 1)".
- The "Introduction to the standard" has been replaced with "Overview"
- The Scope is unchanged.
- The References are unchanged except for IEEE Std 730.1–1989, which has been replaced with IEEE Std 730-1990, both bearing the same title.
- The definitions and acronyms are unchanged.
- The conformance declaration, clause 6.4 (old Section 4.4), has been changed from "IEEE Std 828-1990" to "IEEE Std 828-1998"

- The "Appendix" of 1990 has been changed to "Annex A" of 1998 and the table revised to reflect the new paragraph numbering.
- "Annex B" has been added to the 1998 issue and is an informative guideline for compliance with IEEE/EIA-12207-1997.

In Regulatory Guide 1.169, September 1997, the NRC recognized IEEE Std 828-1990, as providing an approach acceptable to the NRC staff for meeting the requirements of 10 CFR Part 50, as applied to software, in planning configuration management of safety system software, subject to certain provisions. The 1998 revision of IEEE Std 828 did not address these issues. The provisions identified in section C of Regulatory Guide 1.169 remain applicable to the 1998 issue of IEEE Std 828. DCS commits to incorporating the provisions identified in the Regulatory Guide into the MOX facility process control software configuration management plan.

Action:

None

175. Section 11.6.7, p. 11.6-13

Discuss any significant difference (applicable to MOX) between IEEE Standard 830-1998, "IEEE Standard Recommended Practice for Software Requirements Specifications," and the 1993 version of this standard. Discuss how the DCS commitment to IEEE Standard 830-1998 meets the guidance provided in Regulatory Guide 1.172, "Software Requirements Specifications for Digital Computer Software Used in Safety systems of Nuclear Power Plants."

DCS has committed to IEEE Standard 830-1998. The NRC staff, in Regulatory Guide 1.172, has endorsed the 1993 version of this standard.

Per Section 11.3 of the SRP, information is recommended to determine if the design basis adequately addresses the functional requirements for the system. Per Section 11.4.3.2 of the SRP, instrumentation and control systems should be available and reliable and designed with specific considerations such as those contained in IEEE Standard 830 and Regulatory Guide 1.172.

Response:

DCS has compared the two revisions of IEEE Std 830 and have found that the technical requirements and content of IEEE Std 830-1993 are the same as the technical requirements and content of IEEE Std 830-1998. The textual content of the two issues is very nearly identical.

The differences are as follows:

- The 1998 issue adds a second informative annex, which discusses the compliance with IEEE/EIA-12207.1-1997.
- The titles and identifying numbers of referenced documents have been updated.
- IEEE Std 830 (1993 or 1998) establishes recommended methods for specifying software requirements. The practice of, and process of, specifying software requirements is independent of the intended user or application the software and as such this document makes no mention of the application of the software.

For the implementation of IEEE Std 830, DCS will include the NRC's exceptions to the standard listed in section C of Regulatory Guide 1.172, *"Software Requirements Specifications for Digital Computer Software Used in Safety systems of Nuclear Power Plants."*

Action:

None

176. Section 11.6.7, p. 11.6-13

Discuss any significant difference (applicable to MOX) between IEEE Standard 1012-1998, "IEEE Standard for the Software Verification and Validation," and the 1986 version of this standard. Discuss how the DCS commitment to IEEE Standard 1012-1998 meets the guidance provided in Regulatory Guide 1.168, "Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants."

DCS has committed to IEEE Standard 1012-1998. The NRC staff, in Regulatory Guide 1.168, has endorsed the 1986 version of this standard.

Per Section 11.3 of the SRP, information is recommended to determine if the design basis adequately addresses the functional requirements for the system. Per Section 11.4.3.2 of the SRP, instrumentation and control systems should be available and reliable and designed with specific considerations such as those contained in IEEE Standard 1012 and RG 1.168.

Response:

The 1986 issue of IEEE Std 1012 established requirements for the form and content of software V&V plans. This is still provided, although with additional and more detailed requirements, in the 1998 issue of the standard. The 1998 issue of the standard includes additional information that appears in Section 5, "V&V processes", and Section 6, "Software V&V reporting, administrative, and documentation requirements," which provide the requirements and practices for actualizing the V&V plan.

The form of IEEE Std 1012-1998 has changed significantly from IEEE Std 1012-1986.

The title of the 1986 issue was "IEEE Standard for Software Verification and Validation Plans." The title of the 1998 issue is "IEEE Standard for Software Verification and Validation."

The change in the content of IEEE Std 1012 is described in the introduction to the 1998 issue and is stated as follows:

> "IEEE Std 1012-1986 was a product standard that defined the contents of the Software Verification and Validation Plan (SVVP). This revision of the standard, IEEE Std 1012-1998, is a process standard that defines the verification and validation processes in terms of specific activities and related tasks. IEEE Std 1012-1998 also defines the contents of the SVVP including example format".

A new section has been added to the 1998 issue of the standard, section 4, titled "V&V software integrity levels."

Section 3 of the 1986 issue described the required content off the V&V plan. This section has been moved into Section 7 of the 1998 issue. The detailed requirements of the plan are still located in Table 1, which is found in both issues of the standard. While the description of the required contents of the plan as described in the 1986 issue can still be found largely intact in Section 7 of the 1998 issue, the 1998 issue has relocated some parts of the 1986 text within

Section 7 and added a significant body of additional, detailed requirements that are not found in the 1986 issue.

By comparing the outline of the plan as suggested in the 1986 issue with the outline of the plan as suggested in the 1998 issue, the areas of change can be noted.

From IEEE Std 1210-1986	**From IEEE Std 1210-1998**
Software Verification and Validation Plan Outline	Software V&V plan outline (example)
1. Purpose	1. Purpose
2. Referenced Documents	2. Referenced Documents
3. Definitions	3. Definitions
4. Verification and Validation Overview	4. V&V Overview
4.1 Organization	4.1 Organization
4.2 Master Schedule	4.2 Master Schedule
	4.3 Software Integrity Level Scheme
4.3 Resources Summary	4.4 Resources Summary
4.4 Responsibilities	4.5 Responsibilities
4.5 Tools, Techniques, and Methodologies	4.6 Tools, Techniques, and Methods
5. Life-Cycle Verification and Validation	5. V&V Processes
5.1 Management of V&V	5.1 Process: Management
	5.1.1 Activity: Management of V&V
	5.2 Process: Acquisition
	5.2.1 Activity: Acquisition Support V&V
	5.3 Process: Supply
	5.3.1 Activity: Planning V&V
	5.4 Process: Development
5.2 Concept Phase V&V	5.4.1 Activity: Concept V&V
5.3 Requirements Phase V&V	5.4.2 Activity: Requirements V&V
5.4 Design Phase V&V	5.4.3 Activity: Design V&V
5.5 Implementation Phase V&V	5.4.4 Activity: Implementation V&V
5.6 Test Phase V&V	5.4.5 Activity: Test V&V
5.7 Installation and Checkout Phase V&V	5.4.6 Activity: Installation and Checkout V&V
5.8 Operation and Maintenance Phase V&V	5.5 Process: Operation
	5.5.1 Activity: Operation V&V
	5.6 Process: Maintenance
	5.6.1 Activity: Maintenance V&V
6 Software V&V reporting	6. V&V Reporting Requirements
7. V&V Administrative Procedures	7. V&V Administrative Requirements
7.1 Anomaly Reporting and Resolution	7.1 Anomaly Resolution and Reporting
7.2 Task Iteration Policy	7.2 Task Iteration Policy
7.3 Deviation Policy	7.3 Deviation Policy
7.4 Control Procedures	7.4 Control Procedures
7.5 Standards, Practices, and Conventions	7.5 Standards, Practices, and Conventions
	8. V&V Documentation Requirements

In Regulatory Guide 1.168, September 1997, the NRC recognized IEEE Std 1012-1986 as providing an approach acceptable to the NRC staff for meeting the requirements of 10 CFR Part 50 and the guidance given in Revision 1 of Regulatory Guide 1.152, "Criteria for Digital Computers in Safety Systems of Nuclear Power Plants," as they apply to the verification and validation of safety system software, subject to the exceptions identified in Sections C1 through C8 and C11 of the Regulatory Guide. The NRC's exception generally pertains to applications of an Appendix B QA program to the V&V process. The 1998 revision of IEEE Std 1012 did not address these issues. The exceptions remain applicable to the 1998 issue of IEEE Std 1012. DCS commits to incorporating the provisions identified in the Regulatory Guide into the verification and validation of safety system software for the MOX facility.

Action:

None

177. Section 11.6.7, p. 11.6-13

Discuss any significant difference (applicable to MOX) between IEEE Standard 1028-1997, "IEEE Standard for Software Reviews," and the 1988 version of this standard. Discuss how the DCS commitment to IEEE Standard 1028-1997 meets the guidance provided in Regulatory Guide 1.168.

DCS has committed to IEEE Standard 1028-1997. The NRC staff, in Regulatory Guide 1.168, has endorsed the 1988 version of this standard.

Per Section 11.3 of the SRP, information is recommended to determine if the design basis adequately addresses the functional requirements for the system. Per Section 11.4.3.2 of the SRP, instrumentation and control systems should be available and reliable and designed with specific considerations such as those contained in IEEE Standard 1028 and RG 1.168.

Response:

The intent of the 1997 version remains the same as the 1988 version; however, the content has been rearranged and a substantial amount of detailed requirements and implementing procedure and detail has been added.

Summary of changes

The title of the 1997 version has been changed to "IEEE Standard for Software Reviews." The title of the 1988 version was "IEEE Standard for Software Reviews and Audits."

The general arrangement of the standard is unchanged. The reference documents within the standard have been brought up to date.

The 1998 (new) issue of the procedure provides detailed, prescriptive instructions and procedures for performing software reviews and audits. The new issue identifies specific individuals, groups, organizations and management levels and assigns specific responsibilities, actions, and tasks to those entities. The new issue prescribes the expected output of each entity and prescribes the form and required content of the output.

The following table is a comparison of the sections of the 1988 and the 1997 versions of IEEE Std 1028.

IEEE Std 1028 - 1988	IEEE Std 1028 - 1997
4 Management Review Process	4 Management reviews
4.1 Objective	4.1 Introduction
4.2 Abstract	4.2 Responsibilities
4.3 Special responsibilities	4.2.1 Decision maker
4.4 Input	4.2.2 Review leader
4.5 Entry criteria	4.2.3 Recorder
4.5.1 Authorization	4.2.4 Management staff
4.5.2 Initiating Event	4.2.5 Technical staff
4.6 Procedures	4.2.6 Customer or user representative
4.6.1 Planning	4.3 Input
4.6.2 Overview	4.4 Entry criteria
4.6.3 Preparation	4.4.1 Authorization
4.6.4 Examination	4.4.2 Preconditions
4.6.5 Rework	4.5 Procedures
4.7 Exit criteria	4.5.1 Management preparation
4.8 Output	4.5.2 Planning the review
4.9 Auditability	4.5.3 Overview of review procedures
	4.5.4 Preparation
	4.5.5 Examination
	4.5.6 Rework/follow-up
	4.6 Exit criteria
	4.7 Output

IEEE Std 1028 - 1988	IEEE Std 1028 - 1997
5 The Technical Review Process	5 Technical reviews
5.1 Objective	5.1 Introduction
5.2 Abstract	5.2 Responsibilities
5.3 Special responsibilities	5.2.1 Decision maker
5.3.1 Leader	5.2.2 Review leader
5.3.2 Recorder	5.2.3 Recorder
5.3.3 Team member	5.2.4 Technical staff
5.4 Input	5.2.5 Management staff
5.5 Entry criteria	5.2.6 Customer or user representative
5.5.1 Authorization	5.3 Input
5.5.2 Initiating Event	5.4 Entry criteria
5.6 Procedures	5.4.1 Authorization
5.6.1 Planning	5.4.2 Preconditions
5.6.2 Overview	5.5 Procedures
5.6.3 Preparation	5.5.1 Management preparation
5.6.4 Examination	5.5.2 Planning the review
5.7 Exit criteria	5.5.3 Overview of review procedures
5.8 Output	5.5.4 Overview of the software product
5.9 Auditability	5.5.5 Preparation
	5.5.6 Examination
	5.5.7 Rework/follow-up
	5.6 Exit criteria
	5.7 Output

IEEE Std 1028 - 1988	IEEE Std 1028 - 1997
6 The Software Inspection Process	6 Inspections
6.1 Objective	6.1 Introduction
6.2 Abstract	6.2 Responsibilities
6.3 Special responsibilities	6.2.1 Inspection leader
6.3.1 Moderator	6.2.2 Recorder
6.3.2 Reader	6.2.3 Reader
6.3.3 Recorder	6.2.4 Author
6.3.4 Inspector	6.2.5 Inspector
6.3.5 Author	6.3 Input
6.4 Input	6.4 Entry criteria
6.5 Entry criteria	6.4.1 Authorization
6.5.1 Authorization	6.4.2 Preconditions
6.5.2 Initiating Event	6.4.3 Minimum entry criteria
6.5.3 Minimum Entry Criteria	6.5 Procedures
6.6 Procedures	6.5.1 Management preparation
6.6.1 Planning	6.5.2 Planning the inspection
6.6.2 Overview	6.5.3 Overview of inspection procedures
6.6.3 Preparation	6.5.4 Preparation
6.6.4 Examination	6.5.5 Examination
6.6.4.1 Introduce meeting	6.5.5.1 Introduce meeting
6.6.4.2 Establish preparedness	6.5.5.2 Establish preparedness
6.6.4.3 Review the inspection checklist	6.5.5.3 Review general items
6.6.4.4 Read software elements and record defects	6.5.5.4 Review software product and record anomalies
6.6.4.5 Review the defect list	6.5.5.5 Review the anomaly list
6.6.4.6 Make exit decision	6.5.5.6 Make exit decision
6.6.5 Rework	6.5.6 Rework/follow-up
6.6.6 Follow-up	6.6 Exit criteria
6.7 Exit criteria	6.7 Output
6.8 Output	6.8 Data collection recommendations
6.9 Auditability	6.8.1 Anomaly classification
6.10 Data collection requirements	6.8.2 Anomaly classes
6.10.1 Defect type	6.8.3 Anomaly ranking
6.10.2 Defect class	6.9 Improvement
6.10.3 Additional defect classes	
6.10.4 Defects ranked by severity	

IEEE Std 1028 - 1988	**IEEE Std 1028 - 1997**
7 The Walk through process	7 Walk throughs
7.1 Objective	7.1 Introduction
7.2 Abstract	7.2 Responsibilities
7.3 Special responsibilities	7.2.1 Walk-through leader
7.3.1 Moderator	7.2.2 Recorder
7.3.2 Recorder	7.2.3 Author
7.3.3 Author	7.3 Input
7.4 Input	7.4 Entry criteria
7.5 Entry criteria	7.4.1 Authorization
7.5.1 Authorization	7.4.2 Preconditions
7.5.2 Initiating Event	7.5 Procedures
7.6 Procedures	7.5.1 Management preparation
7.6.1 Planning	7.5.2 Planning the walk-through
7.6.2 Overview	7.5.3 Overview
7.6.3 Preparation	7.5.4 Preparation
7.6.4 Examination	7.5.5 Examination
7.7 Exit criteria	7.5.6 Rework/follow-up
7.8 Output	7.6 Exit criteria
7.9 Auditability	7.7 Output
	7.8 Data collection recommendations
	7.8.1 Anomaly classification
	7.8.2 Anomaly classes
	7.8.3 Anomaly ranking
	7.9 Improvement

IEEE Std 1028 - 1988	IEEE Std 1028 - 1997
8 The audit process	8. Audits
8.1 Objective	8.1 Introduction
8.2 Abstract	8.2 Responsibilities
8.3 Special responsibilities	8.2.1 Lead auditor
8.4 Input	8.2.2 Recorder
8.5 Entry criteria	8.2.3 Auditor
8.6 Procedures	8.2.4 Initiator
8.6.1 Planning	8.2.5 Audited organization
8.6.2 Overview	8.3 Input
8.6.3 Preparation	8.4 Entry criteria
8.6.4 Examination	8.4.1 Authorization
8.6.5 Reporting	8.4.2 Preconditions
8.7 Exit criteria	8.5 Procedures
8.8 Output	8.5.1 Management preparation
8.9 Auditability	8.5.2 Planning the audit
	8.5.3 Opening meeting
	8.5.4 Preparation
	8.5.5 Examination
	8.5.5.1 Evidence collection
	8.5.5.2 Closing meeting
	8.5.5.3 Reporting
	8.5.6 Follow-up
	8.6 Exit criteria
	8.7 Output

As can be seen from a comparison of the two versions, the major sections (4, 5, 6, 7, and 8) are preserved. Within each section, the subsections and most of the lower subsections are also preserved. However, within the subsections and below, the new standard provides a finer specification of the required activities and establishes a clearly prescribed set of activities and criteria for performing a review or audit. The new issue has also added additional subsections that provide detailed and precise requirements.

DCS has chosen to use the new issue because the new issue reduces ambiguity of the requirements for how to perform a review, or what is required in a review, or who is responsible for doing what in a review. The new issue clearly describes how to conduct software reviews and audits.

In Regulatory Guide 1.168, September 1997, the NRC recognized IEEE Std 1028-1988 as providing an approach acceptable to the NRC staff for carrying out software reviews, inspections, walkthroughs, and audits, subject to the exceptions identified in Sections C9 through C11 of the Regulatory Guide. The 1997 revision of IEEE Std 1028 did not address these issues. The exceptions remain applicable to the 1997 issue of IEEE Std 1028. DCS commits to incorporating the provisions identified in the Regulatory Guide when planning and conducting software reviews, inspections, walkthroughs, and audits of the MOX safety system software.

Action:

None

178. <u>Section 11.6.7, p. 11.6-13</u>

Discuss any significant difference (applicable to MOX) between IEEE Standard 1074-1997, "IEEE Guide for Developing Software Life Cycle Processes," and the 1995 version of this standard. Discuss how the DCS commitment to IEEE Standard 1074-1997 meets the guidance provided in Regulatory Guide 1.173, "Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants." Discuss MOX computer software life cycle activities in light of the guidance contained in Branch Technical Position (BTP) HICB-14 contained in NUREG-0800.

DCS has committed to IEEE Standard 1074-1997. The NRC staff, in Regulatory Guide 1.173, has endorsed the 1995 version of this standard. Also, BTP HICB-14 in NUREG-0800 provides guidance on software life cycle activities for digital computer-based instrumentation and control systems.

Per Section 11.3 of the SRP, information is recommended to determine if the design basis adequately addresses the functional requirements for the system. Per Section 11.4.3.2 of the SRP, instrumentation and control systems should be available and reliable and designed with specific considerations such as those contained in IEEE Standard 1074, RG 1.173, and BTP HICB-14.

Response:

IEEE Std 1074-1997, "IEEE Guide for Developing Software Life Cycle Processes," provides a structure for developing a software life cycle model that has been recognized in NUREG/CR-6101 and BTP HICB-14.

The 1997 issue of IEEE Std 1074 is essentially unchanged in its intent and requirements from the 1995 issue.

Both the 1995 and the 1997 issues list 65 activities that are grouped into 17 activity groups that must be performed to generate a satisfactory lifecycle process. The term "activity group" is used in the 1997 issue of the standard and it replaces the term "process," which was used in the 1995 issue of the standard. The format of each activity remains unchanged: input information, description, and output information.

The 1997 issue has changed the format of the standard. Sections 3 through 7, which contained the actual "processes" of the 1995 issue have been relocated to normative Annex A of the 1997 issue.

The 1997 issue has added an "activity group" establishing processes for risk management and an "activity group" addressing the process of "importing" software from an external source.

Section 3.3, Software Quality Management Process, of the 1995 issue does not directly map into any single part of the 1997 issue although there are activities in section A1.1 of the 1997 issue (plan project management, define metrics) that are applicable to the implementation of a software quality management plan. However, software quality management is the subject of IEEE Std 730, "IEEE Standard for Software Quality Assurance Plans."

The 1997 issue of the standard provides an exact and detailed set of instructions and steps that are required to be performed to establish a lifecycle plan. Each of the activities is meticulously specified in the 1997 issue and as such, it is more prescriptive than the 1995 issue of the standard.

Comparing the structure of the 1995 issue of IEEE Std 1074 with the 1997 issue. The following table maps the structure of the 1995 issue of IEEE Std 1074 into the structure of the 1997 issue of the standard.

IEEE Std 1074 - 1995	**IEEE Std 1074 - 1997**
1. Overview 1.1 Scope 1.5 Use of this standard 1.4 Organization of this document	1. Overview 1.1 Scope 1.2 Purpose 1.3 Product of standard 1.4 Intended audiences 1.5 Relationship to other key standards 1.6 Relationship to process improvement 1.7 Organization of this standard
1.2 References	2. References
1.3 Definitions and acronyms	3. Definitions and acronyms 3.1 Definitions 3.2 Acronyms
	4. Key concepts 4.1 Activities 4.2 Elements of the SLCP 4.3 Mapping 4.4 Input Information and Output Information
2. Software Life Cycle Model Process 2.1 Overview 2.2 Activities List 2.3 Identify Candidate Life cycle models 2.4 Select Project Model	5. Implementation of the standard 5.1 Select an SLCM 5.2 Create an SLC 5.3 Establish an SLCP
 3. Project Management Process 3.1 Project Initiation Process	Annex A (normative) Activities A.1 Project Management Activity Groups A.1.1 Project Initiation Activities A.1.1.1 Create SLCP A.1.1.2 Perform Estimations A.1.1.3 Allocate Project Resources A.1.1.4 Define Metrics

IEEE Std 1074 - 1995	**IEEE Std 1074 - 1997**
	A.1.2 Project Planning Activities A.1.2.1 Plan Evaluations A.1.2.2 Plan Configuration Management A.1.2.3 Plan System Transition (If Applicable) A.1.2.4 Plan Installation A.1.2.5 Plan Documentation A.1.2.6 Plan Training A.1.2.7 Plan Project Management A.1.2.8 Plan Integration
3.2 Project Monitoring and Control Process	A.1.3 Project Monitoring and Control Activities A.1.3.1 Manage Risks A.1.3.2 Manage the Project A.1.3.3 Identify SLCP Improvement Needs A.1.3.4 Retain Records A.1.3.5 Collect and Analyze Metric Data
3.3 Software Quality Management Process	
4. Pre-development process 4.1 Concept exploration process	A.2 Pre-Development Activity Groups A.2.1 Concept Exploration Activities A.2.1.1 Identify Ideas or Needs A.2.1.2 Formulate Potential Approaches A.2.1.3 Conduct Feasibility Studies A.2.1.4 Refine and Finalize the Idea or Need
4.2 System allocation process	A.2.2 System Allocation Activities A.2.2.1 Analyze Functions A.2.2.2 Develop System Architecture A.2.2.3 Decompose System Requirements
	A.2.3 Software Importation Activities A.2.3.1 Identify Imported Software Requirements A.2.3.2 Evaluate Software Import Sources (If Applicable) A.2.3.3 Define Software Import Method (If Applicable) A.2.3.4 Import Software (If Applicable)
5. Development process 5.1 Requirements process	A.3 Development Activity Groups A.3.1 Requirements Activities A.3.1.1 Define and Develop Software Requirements A.3.1.2 Define Interface Requirements A.3.1.3 Prioritize and Integrate Software Requirements

IEEE Std 1074 - 1995	IEEE Std 1074 - 1997
5.2 Design process	A.3.2 Design Activities A.3.2.1 Perform Architectural Design A.3.2.2 Design Data Base (If applicable) A.3.2.3 Design Interfaces A.2.3.4 Perform Detailed Design
5.3 Implementation process	A.3.3 Implementation Activities A.3.3.1 Create Executable Code A.3.3.2 Create Operating Documentation A.3.3.3 Perform Integration
6 Post-development Process 6.1 Installation process	A.4 Post-Development Activity Groups A.4.1 Installation Activities A.4.1.1 Distribute Software A.4.1.2 Install Software A.4.1.3 Accept Software in Operational Environment
6.2 Operation and support process	A.4.2 Operation and Support Activities A.4.2.1 Operate the System A.4.2.2 Provide Technical Assistance and Consulting A.4.2.3 Maintain Support Request Log
6.3 Maintenance process	A.4.3 Maintenance Activities A.4.3.1 Identify Software Improvement Needs A.4.3.2 Implement Problem Reporting Method A.4.3.3 Reapply SLC
6.4 Retirement process	A.4.4 Retirement Activities A.4.4.1 Notify User A.4.4.2 Conduct Parallel Operations (If Applicable) A.4.4.3 Retire System
7 Integral process 7.1 Verification and validation process	A.5 Integral Activity Groups A.5.1 Evaluation Activities A.5.1.1 Conduct Reviews A.5.1.2 Create Traceability Matrix A.5.1.3 Conduct Audits A.5.1.4 Develop Test Procedures A.5.1.5 Create Test Data A.5.1.6 Execute Tests A.5.1.7 Report Evaluation Results

IEEE Std 1074 - 1995	IEEE Std 1074 - 1997
7.2 Software Configuration Management process	A.5.2 Software Configuration Management Activities A.5.2.1 Develop Configuration Identification A.5.2.2 Perform Configuration Control A.5.2.3 Perform Status Accounting
7.3 Documentation development process	A.5.3 Documentation Development Activities A.5.3.1 Implement Documentation A.5.3.2 Produce and Distribute Documentation
7.4 Training process	A.5.4 Training Activities A.5.4.1 Develop Training Materials A.5.4.2 Validate the Training Program A.5.4.3 Implement the Training Program

In Regulatory Guide 1.173, September, 1997, the NRC recognized IEEE Std 1074-1995, "IEEE Standard for Developing Software Life Cycle Processes," as providing an approach acceptable to the NRC staff for meeting the requirements of 10 CFR Part 50 and the guidance in Revision 1 of Regulatory Guide 1.152, "Criteria for Digital Computers in Safety Systems of Nuclear Power Plants," as they apply to development processes for safety system software, subject to the provisions listed in section C1 through C6 of the Regulatory Guide. The 1997 revision of IEEE Std 1074 did not address these issues. The exceptions remain applicable to the 1997 issue of IEEE Std 1074. DCS commits to incorporating the provisions identified in the Regulatory Guide when developing lifecycle plans and models for the MOX safety system software.

Action:

None

179. <u>Section 11.6.7, pp. 11.6-12 thru 11.6-14</u>

Discuss the use and qualification of isolation devices for the MOX facility in light of the guidance contained in BTP HICB-11 in NUREG-0800.

Branch Technical Position HICB-11 in NUREG-0800 provides guidance on isolation devices.

Per Section 11.3 of the SRP, information is recommended to determine if the design basis adequately addresses the functional requirements for the system. Per Section 11.4.3.2 of the SRP, instrumentation and control systems should be available and reliable and designed with specific considerations such as those contained in BTP HICB-11.

Response:

Isolation devices will be used in the design of the MFFF. Isolation devices will be used to maintain the electrical and physical separation between the normal control system and the protection system, the safety system and both channels of the emergency systems to ensure that redundancy and independence are maintained. Branch Technical Position HCIB-11 provides the NRC's position on qualification testing of isolation devices. This includes developing an acceptable test program and identifies the appropriate industry standards in which the test conditions and methods are detailed.

Isolation devices will be designed and qualified to provide isolation between redundant principal SSCs or between principal SSCs and non-principal SSCs from the application of maximum credible faults, short circuits, open circuits, and grounds. DCS is committed to maintain independence of redundant safety and non-safety systems per the requirements of IEEE Std 384-1992.

The maximum credible fault will be determined by analysis. The maximum credible fault will be established based on proximity of circuits, faults, human error, natural phenomena (lightning) and switching transients. Surge withstand waveforms will be developed using IEEE Std C62.41-1991, "IEEE Recommended Practice on Surge Voltages in Low-Voltage AC Power Circuits."

Testing or analysis will be used to qualify isolation devices. The industry standards identified in BTP HCIB-11 will be used as the basis for qualification testing of isolation devices.

Action:

None

180. <u>Section 11.6.7, p. 11.6-14</u>

Discuss how the DCS commitment to Instrument Society of America (ISA) 67.04.01-2000, "Setpoints for Nuclear Safety-Related Instrumentation," meets the guidance contained in BTP HICB-12 of NUREG-0800 and Regulatory Guide 1.105, "Instrument Setpoints for Safety-Related Systems."

DCS has committed to ISA 67.04.01-2000. Branch Technical Position HICB-12 in NUREG-0800 and Regulatory Guide 1.105 provide guidance on establishing and maintaining instrument setpoints.

Per Section 11.3 of the SRP, information is recommended to determine if the design basis adequately addresses the functional requirements for the system. Per Section 11.4.3.2 of the SRP, instrumentation and control systems should be available and reliable and utilize specific design considerations such as those contained in ISA 67.04.01-2000, Regulatory Guide 1.105, and BTP HICB-12.

Response:

In revision 3 of Regulatory Guide 1.105, issued in December 1999, the staff has endorsed the setpoint development practice identified in ANSI/ISA-S67.04-1994: Setpoints for Nuclear Safety-Related Instrumentation, for developing safety related setpoints. The staff identified four caveats to their recognition. The ISA recently revised S67.04-Part I-1994. The new identification is ANSI/ISA S67-04.01-2000. The ISA now identifies the internal sections of the standard with the term "clause" rather than the older term "section." Street addresses of referenced standards bodies have been updated. The technical content of the 2000 issue of the standard remains identical to the 1994 issue.

Branch Technical Position HCIB-12 also recognizes ISA-S67.04 Part I.

For the development of setpoints for IROFS, DCS has committed to ANSI/ISA-S67.04.01-2000.

Because the content of the 2000 issue of the standard is identical to the 1994 issue, the four caveats the Staff applied to the 1994 issue are still applicable.

By committing to the practices identified in ANSI/ISA-S67.04.01-2000, which have been endorsed by the Staff, the instrument spans, setpoints, and control ranges for instrumentation and control IROFS will be available and reliable.

Action:

None

181. <u>Section 11.6.7, pp. 11.6-12 thru 11.6-14</u>

Discuss the self-test and surveillance test provisions for MOX instrumentation and control systems in light of BTP HICB-17 contained in NUREG-0800.

BTP HICB-17 in NUREG-0800 provides guidance on self-test and surveillance test provision for digital computer-based instrumentation and control systems.

Per Section 11.3 of the SRP, information is recommended to determine if the design basis adequately addresses the functional requirements for the system. Per Section 11.4.3.2 of the SRP, instrumentation and control systems should be available and reliable and designed with specific considerations such as those contained in BTP HICB-17.

Response:

The IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations, IEEE Std 603, Section 5.7, Capability for Testing and Calibration, requires that the design provide the capability of testing and calibration of safety system equipment while retaining the capability of the safety system to accomplish its safety function. DCS will comply with this.

This commitment conforms to the acceptance criteria of Branch Technical Position HICB-17, page 17-4. The ability to perform self-testing and provide design features that facilitate surveillance testing will be provided. As the design is developed, these specific features will be identified.

Self test and monitoring capability, including such continuous test and monitoring routines as "pulse monitoring" and "watchdog timers" is normally a standard feature of software programmable electronic systems used in industrial applications. The implementation of such monitoring is dependent on the particular hardware and software selected for the design. As the design is developed, these features will be identified.

DCS has committed to the single failure criterion in CAR Section 5.5.5.2. For Electrical and Instrument and Controls Systems in Sections 11.5 and 11.6 of the CAR, DCS has committed specifically to IEEE Std 379-1994, "IEEE Standard Application of the Single Failure Criterion to Nuclear Generating Station Safety Systems." IEEE Std 379-1994 stipulates that system design should be such that all active failures related to IROFS are detectable. DCS will perform single failure analysis to demonstrate that all active failures are detectable either by surveillance testing, annunciation, or automatic self-testing.

Action:

None

182. Section 11.6.7, pp. 11.6-12 thru 11.6-14

Discuss the use of programmable logic controllers (PLCs) for MOX instrumentation and control systems in light of BTP HICB-18 contained in NUREG-0800.

BTP HICB-18 in NUREG-0800 provides guidance on the use of PLCs in digital computer-based instrumentation and control systems.

Per Section 11.3 of the SRP, information is recommended to determine if the design basis adequately addresses the functional requirements for the system. Per Section 11.4.3.2 of the SRP, instrumentation and control systems should be available and reliable and designed with specific considerations such as those contained in BTP HICB-18.

Response:

The Design Criteria for the control systems in the MFFF that are classified as IROFS will be based on the requirements of the standards identified in the CAR. In the CAR, DCS states that the safety control subsystems and emergency control system will be designed using the methods and practices identified in IEEE Std 603-1998, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations." Software programmable electronic systems used in safety control subsystems are designed using the methods and practices identified in IEEE Std 7-4.3.2-1993, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations." While IEEE Std 603 is specifically applicable to the design of safety systems found in nuclear power plants, the safety system design basis identified in Section 4, paragraphs (a) through (l) are applicable to the IROFS that are found in the MFFF, recognizing that there are conditions, systems, operating requirements and consequences unique to a nuclear plant and not found in a fuel fabrication facility. Similarly, the criteria for safety systems identified in Section 5 of IEEE Std 603, while specifically applicable to a nuclear power plant, are also applicable to the IROFS that are found in the MFFF.

IEEE Std 7-4.3.2 is an extension of IEEE Std 603 and provides requirements unique to software programmable electronic systems, which includes digital computers, used in safety systems. The safety system design basis, Section 4, and the safety system criteria, Section 5, of IEEE Std 7-4.3.2 are generally applicable to the IROFS found in the MFFF. Again, recognizing that they are conditions, systems, operating requirements and consequences unique to a nuclear plant and not found in a fuel fabrication facility.

IEEE Std 7-4.3.2, Section 5.3.2, Qualification of existing commercial computers, establishes the requirements for qualifying software for use in a safety system in a nuclear power plant and identifies acceptable methods for establishing the qualification. This is the subject of much of NUREG/CR-6421 and EPRI TR106439 identified in branch technical position HICB-18. DCS will use EPRI TR106439 as the guideline for qualification of programmable logic controllers.

IEEE Std 7-4.3.2, Section 5.3.1, Software development, and Section 5.3.4, Verification and validation, both establish requirements that software shall be developed in accordance with a disciplined and controlled software development program and an approved QA plan. This is the subject of NUREG/CR-6090 and branch technical position HCIB-14.

NUREG/CR-6090 is intended to provide guidance to those who review the application of software programmable electronic systems in safety systems in a nuclear power plant, not to those who would be designing the application. It is however useful to the designers to ensure that the designers are aware of the particular concerns of an oversight body.

NUREG/CR-6463 is intended to provide guidance to those who review the application software of a programmable electronic system in safety systems in a nuclear power plant, not to those who would be developing the application. It is however useful to the software application developers to ensure that the developers are aware of the particular concerns of an oversight body.

Action:

None

183. Section 11.7, pp. 11.7-1 thru 11.7-6

Provide a list of specific material handling equipment identified as principle structures, systems, or components (SSCs) and its location in the facility.

Section 11.4.7 of the SRP recommends that information be provided on material transport system design and operation to fulfill all of the functional requirements determined by the integrated safety assessment. The list of the specific subcomponents of the material handling equipment that may be principle SSCs are not provided. This information is needed to clarify the scope and extent of safety significance of the system.

Response:

Material handling equipment, at the system or functional level, is identified as a principal SSC in Chapter 5 of the CAR. The specific components that are IROFS will be identified in the ISA.

To facilitate an understanding of the types of material handling equipment being evaluated, a list of equipment is provided below:

- Various material handling equipment located outside gloveboxes:
  - Receiving and shipping area: monorails, bridge cranes, and conveyors are provided to handle shipping packages (9975 or 9517), UO_2 drums, or 3013 containers. Fresh fuel packages are handled using an air pallet and a bridge crane.
  - AP and MP powder and pellet processing areas: several bridge cranes are provided for glovebox maintenance.
  - Waste area: Bridge-cranes, conveyors, and forklifts are used to handle pallets of 55-gallon waste drums or single drums.
  - Rod area: elevator, gantries, stacker retriever, and trolleys are used to handle either single rods or rod trays.
  - Assembly area: monorails, bridge cranes, and upending fixtures are provided.
- Various handling equipment located inside gloveboxes:
  - AP area: incoming PuO_2 3013 containers or reusable cans are handled using elevators, conveyors, horizontal transfer units, tilter, stacker retriever, (buffer storage) and pneumatic transfers.
  - Powder area: jars and dust pots are handled in casks containing either a jar or a dust pot basket. These casks are handled by trolleys, conveyors and elevators. Jars are also handled by tilters.

- Pellet area: pellets are handled in Mo boats; scrapped pellets or dust pots are handled in stainless steel boxes. Grinded or sorted pellets are then handled in trays, themselves stacked to form tray baskets. These containers are handled by elevators, tilters, conveyors, horizontal transfer units, stacker retrievers (storages), and rotating tables. Single pellets are handled by conveyors, vibrating rails, and robots.

- Rod area: rods are handled by conveyors and wheel tracks.

Action:

None

184. Section 11.7, pp. 11.7-1 thru 11.7-6

Describe the capacity of the material handling equipment during normal operating and accident conditions.

Section 11.4.7.2.A of the SRP recommends that the applicant demonstrate that adequate capacity exists to handle the expected volume of radioactive material during normal operation and accident conditions. This section applies to the specific design considerations for the material handling equipment in general and to parts of the material handling equipment identified as principle SSCs, in particular. Information describing the capacity of the material handling equipment during normal operating and accident conditions was not provided in the application.

Response:

The SRP indicates that one of the criteria for determining acceptability of the design and operation of material transport systems identified as IROFS is demonstrating that adequate capacity exists to handle the expected volume of radioactive material during normal operating and accident conditions. Information regarding the capacity of process material handling equipment, in general, and those portions of process material handling equipment identified as principal SSCs, in particular, is presented below.

Capacities for MFFF material handling equipment vary based on the importance to safety of the function performed by the equipment, by the codes and standards used to design and qualify the equipment, and by project specific design criteria applied to different types of equipment.

Material handling equipment classified as principal SSCs must retain its load during all credible accidents and design basis natural phenomena events, including the design earthquake (DE). The seismic demand associated with the DE is much greater than the seismic demand placed on non-principal SSCs. Therefore, the capacity of principal SSCs, which is related to their ability to withstand seismic loading, is potentially greater than that of non-principal SSCs. Capacity differences vary based on the ratio of the seismic demand to the stress based acceptance criteria from the design code applied to each SSC.

Design codes applied to process material handling equipment where loads are suspended from flexible cables differ from the design codes applied to equipment where loads are carried along fixed geometry tracks. Equipment where loads are suspended is designed using bridge crane, underhung monorail, and hoist codes. These design codes include a minimum safety factor of 5 between the rated capacity of the equipment and the ultimate material strength of load suspension components or nominal breaking strength of wire rope. Process hoisting equipment classified as a principal SSC is further de-rated in accordance with the component specific safety factors from NUREG-0554 applicable to single failure proof cranes for nuclear power plants. Process hoisting equipment used during maintenance activities is restricted to lifting a maximum of 65% of its rated capacity, in accordance with project specific design criteria.

Equipment that lifts loads using lifting devices that run on fixed geometry tracks is qualified to perform their load retention functions in accordance with structural design codes. Fixed geometry handling equipment classified as a principal SSC is qualified in accordance with the loading combinations and acceptance criteria provided in the AISC N690 structural design code. Other fixed geometry handling equipment is qualified in accordance with the AISC Manual of Steel Construction. In addition to design code requirements, project specific design criteria requires that load retention components used in fixed geometry handling equipment vertical lift applications be sized using a minimum safety factor of 3 between the rated load and failure load.

Specific capacities and IROFS will be determined as part of final design and described in the ISA summary.

Action:

None

185. Section 11.7, pp. 11.7-1 thru 11.7-6

Other than the structural design of the system that would prevent failure of the material handling equipment during an event, clarify if other redundancy or diversity in material handling system components is provided to prevent a failure of the system that could lead to a confinement breach.

Section 11.4.7.2.B of the SRP recommends that the application describe equipment diversity or redundancy provided to prevent a system breach. This section applies to the specific design considerations for the material handling equipment in general and to parts of the material handling equipment identified as principle SSCs, in particular. The application does not address redundancy or diversity in design for the material handling equipment.

Response:

The material handling equipment design provides provisions for the retention of any load capable of breaching confinement in case of mechanical system failure or seismic event. Design provisions for material handling equipment located inside a glovebox include the following:

- Redundant brakes on lifting equipment, which actuate on loss of electrical power, overspeed, overtorque, or overtravel
- Structural oversizing of specific mechanical drive related components
- Overspeed detection that isolates electrical power to the motor drive and actuates the safety brake
- Overtorque detection, which stops the lifting motion to avoid any mechanical breakage with the glovebox boundary or any other component inside the glovebox.
- Mechanical stops to prevent over travel of material handling equipment such as conveyors, hoists, tilters, elevators, etc.
- Normal process PLC (Programmable Logic Controller) and electrical interlocks to prevent over travel, mechanical interference, or collisions with other moving equipment.
- Component sizing based on worst case loading combinations, such as the addition of design earthquake loads to loads from equipment operating in the worst case position (e.g., a tilter retaining a full jar in upper vertical position).

Specific IROFS will be confirmed by the ISA as part of detail design.

Action:

None

186. Section 11.7, pp. 11.7-1 thru 11.7-6

Describe the material handling equipment design bases intended to prevent breaches in the glovebox boundary as a result of the normal or off-normal operation of the system. Clarify the statement in Table 5.5-16 regarding the use of "engineered equipment" to prevent material handling equipment from impacting gloveboxes.

Section 11.4.7.2.B of the SRP recommends that information be provided to verify that states that there is redundancy or diversity of components required to prevent the release of radioactive materials to the environment or needed for safe operation of the material transport system. This section applies to the specific design considerations for the material handling equipment in general and to parts of the material handling equipment identified as principle SSCs, in particular. This information on the material handling equipment design bases intended to prevent breaches in the glovebox boundary as a result of the normal or off-normal operation of the system is either not addressed or is unclear as written in the application.

Response:

The material handling equipment safety features intended to prevent breaches in the glovebox boundary are described in the response to Question 185. It will be demonstrated, as part of the detail design, that a load drop inside a glovebox does not lead to a confinement breach.

Safety functions that equipment must perform to maintain confinement are provided below.

- Process equipment that forms a portion of the confinement boundary must maintain structural integrity under loading from all normal operating, credible accident, and design basis natural phenomena conditions.

- Process equipment inside or outside of a glovebox enclosure must not interact with confinement boundary elements during normal operation, credible accident, and design basis natural phenomena condition in such a way as to compromise performance of the confinement function.

- Process equipment inside or outside of a glovebox that supports process containers or other loads capable of breaching the confinement boundary must retain its loads during normal operation, credible accident, and design basis natural phenomena conditions.

Action:

None

187. Section 11.7, pp. 11.7-1 thru 11.7-6

Identify and describe any material handling equipment that is provided with emergency power, if any.

Section 11.4.7.2.C of the SRP recommends that information be provided to should demonstrate provisions for emergency power are included for critical process components. This section applies to the specific design considerations for the material handling equipment in general and to parts of the material handling equipment identified as principle SSCs, in particular. The use of emergency power in the system is not described in the application.

Response:

Material handling equipment are designed to fail safe in case of loss of power. Therefore, emergency power is not required.

Action:

None

188. **Section 11.7, pp. 11.7-1 thru 11.7-6**

Describe how the material handling equipment is designed to minimize buildup of plutonium, uranium, or MOX dust and debris in the transport systems.

Section 11.4.7.2.H of the SRP recommends that information be provided to demonstrate that the equipment is designed to minimize entrapment and buildup of solids in the system. This section applies to the specific design considerations for the material handling equipment in general and to parts of the material handling equipment identified as principle SSCs, in particular. The application does not describe system design to minimize dust and debris buildup.

Response:

Material handling equipment is designed to meet glovebox material requirements and perform its function under dusty conditions. MOX powder, dust, or debris buildup on handling equipment installed inside gloveboxes is limited by design.

Examples of provisions to minimize buildup of powder, dust or debris are:

- Use of design configurations to minimize powder/dust retention
- Mounting of a stainless steel casing to prevent powder/dust retention. This provision may be used for material handling support structures, for example.
- Easily visible and accessible parts for cleaning or maintainability (to access dust/powder)
- Use of sealed bearings or leak-free coupling mechanisms, when appropriate
- Use of appropriate surface quality or coating to facilitate cleaning
- Use of portable vacuum cleaner (or of glovebox vacuum network for some of the equipped powder processing gloveboxes).

Action:

None

189. Section 11.7, pp. 11.7-1 thru 11.7-6

Provide design basis decontamination characteristics for the material handling equipment.

Section 11.4.7.2.J of the SRP recommends that information be provided to verify that materials have surface finishes that have satisfactory decontamination characteristics. This section applies to the specific design considerations for the material handling equipment in general and to parts of the material handling equipment identified as principle SSCs, in particular. Decontamination characteristics for the material handling equipment are not discussed in the application.

Response:

There are no safety significant decontamination characteristics associated with material handling equipment. However, design characteristics for decontamination of material handling equipment include:

- Inside gloveboxes, material handling devices are mostly made of stainless steel with appropriate surface quality to allow decontamination. Appropriate surface qualities such as: N6 or better for inner components and N4 for material in contact with powder. Use of components requiring painting is minimized. Decontamination ability for parts that are painted. Corrosion of carbon steel parts that cannot be stainless steel or painted for functional reasons is prevented by having nitrogen or dry air inside GBs. Inaccessible parts are avoided. Components are designed to be easily accessible and easily dismantled for decontamination. Lubricant use is limited to the extent practical. Various other provisions are taken, such as internal welds are continuous and ground smooth, re-entrant corners have large radius; powder-handling channels are sealed to the extent practical.
- Outside gloveboxes, painting systems will be used for materials located in C3b process rooms to facilitate decontamination.

In addition, mounting operations are carefully performed to prevent surface damage. Once installed onsite, inspection is made and corrective actions are taken to repair any damage.

Action:

None

190. Section 11.8, pp. 11.8-1 thru 11.8-10

Describe the design basis for the fluid transport systems. Provide the design pressures and capacities of the fluid transport systems.

Section 11.4.7.2.A of the SRP recommends that information be provided to verify that adequate capacity exists to handle normal operating and accident conditions. This section applies to the specific design considerations for the fluid transport systems in general and to parts of the fluid transport system equipment identified as principle SSCs, in particular. The NRC needs a clear description of systems, appropriate design bases and values, ranges, control information, needed reliabilities, and identification of any IROFS. The design basis for the fluid transport systems are not provided.

Response:

The Fluid Transport Systems section (CAR Section 11.8) applies to the welded equipment and piping components that are the parts of, and handle the liquid processes for, the MFFF.

For the description of the liquid processes associated with the AP, MOX and utility and reagent unit processes, refer to CAR Sections 11.3, 11.4, and 11.9, respectively. The volumetric capacity basis for the equipment and piping components are defined by the process systems design. The process description Sections 11.3 and 11.4 also cover the required information on volumetric capacity and design basis. Additional design information (pressures, temperatures, etc.) are provided in the response to Question 111.

Refer to the response to Question 39 for information regarding reliabilities/likelihood.

The design criteria used for development of fluid transport system engineering design are as follows:

Design Basis	Design Pressure	Design Temperature	Design Flow & Volumetric Capacities
Storage Tanks	Max value from following: ▪ Pressure (max) in normal operating condition + 10% **OR** ▪ Pressure (max) in normal operating condition + 13 psig or 0.9 bar **OR** ▪ Pressure (max) for transient conditions	Max value from following: ▪ Temp (max) in normal operating condition + 27°F **OR** ▪ Temp (max) for transient conditions	Maximum flow in normal operating conditions + 20%
Process Columns	Same as above	Same as above	Same as above
Exchanger	Same as above	Same as above	Same as above
Pumps	Same as above	Same as above	Same as above
L/P prime movers like air lifts, ejectors, siphons, and etc.	Same as above	Same as above	▪ Process hydraulic calculation
Piping & Valves	Same as above	Same as above	▪ Pipe sizing per line velocity and pressure drop requirements.

Action:

Update Section 11.8.7 Design Basis for principal SSCs with the appropriate content and table from response in the next update of the CAR.

191. **Section 11.8, pp. 11.8-1 thru 11.8-10**

For all fluid transport systems, if a safety function is preventing back-flow into auxiliary systems, describe the applicable design criteria such as type and configuration of check valves. If isolation is safety function, describe the applicable design criteria, such as the type, capability and redundancy in isolation valves.

Section 11.4.7.2.B of the SRP applies to the specific design considerations for the fluid transport systems in general and to parts of the fluid transport system equipment identified as principle SSCs, in particular. No specific description of equipment used to prevent the release of radioactive materials to the environment or needed for safe operation of the system is provided.

Response:

See CAR Section 11.4.1 for a description of confinement features that prevent the release of radioactive materials to the environment.

MFFF process systems are provided with various design features to prevent the backflow of process fluids into associated utility or auxiliary systems. These features that perform safety functions are discussed in the following sections:

Process Vessel Venting

AP processes vessels are vented to the Offgas Treatment System. This design feature prevents pressure perturbations that may result in the backflow of process fluids between pressure vessels.

Transfer Line Design Features

Separator or knockout pots are provided in those lines in which fluid transfer is made by air or vacuum lift. The separator pot body separates the lift mechanism airflow from the process fluid. The separated liquid is allowed to flow by gravity into the desired vessel, while the motive airflow vents at the top of the pot. The vented separator pot prevents back flow siphoning.

Steam jet lift transfer piping is terminated in the receiving vessel vent space, to provide an air gap to prevent siphon and backflow. (Refer to typical schematic)

Siphons are used to initiate gravity transfer of fluids in those applications that do not require flow regulation (e.g., tank emptying). Evacuation of siphon transfer piping causes liquid to raise from the upstream tank to the point at which the liquid begins to flow into the downstream tank by gravity. The relative elevations of the upstream and downstream tanks prevent backflow. The transfer of process fluids by siphon is highly reliable as it requires no moving parts, does not dilute process fluids, and is not prone to clogging.

Hydraulic seals are utilized as a means to prevent backflow of process fluid to the auxiliary systems during reagent addition. The liquid plug or seal is maintained by piping configuration and provides isolation between vessels that are maintained at different ambient pressures. It should be noted that AP process equipment handling radioactive fluids is vented to the Offgas Treatment System.

The hydraulic seal design implements bent "U" type seal tubes or hydraulic seal pots to ensure that:

- The seal remains filled with liquid at all the times.
- The liquid seal withstands the internal pressure of connecting vessels.
- Siphon action is not initiated.

Fully welded intermediate loops are used to supply the process with thermal fluids.

The use of check valves is implemented in plant systems only within the envelope of the process fluid pressure boundary. Check valve response times required to prevent pressure surges and flow reversals are considered in system design. Check valve selection is based upon valve effective pressure drop, type of seating material, pressure and flow reversal response, mounting requirements, and reliable operation and maintenance.

Prevention of flooding in process areas by reagent and utility fluids in the event of earthquake.

The isolation of utility and reagent fluids from the process area is achieved by isolation valves in the piping as it enters the process building. Redundant isolation valves are provided to automatically isolate the fluid lines when earthquake conditions are detected. The isolation valves fail safe to closed position. Isolation valve selection is based on process hydraulics, required control system characteristics, mounting requirements, and other valve specifications.

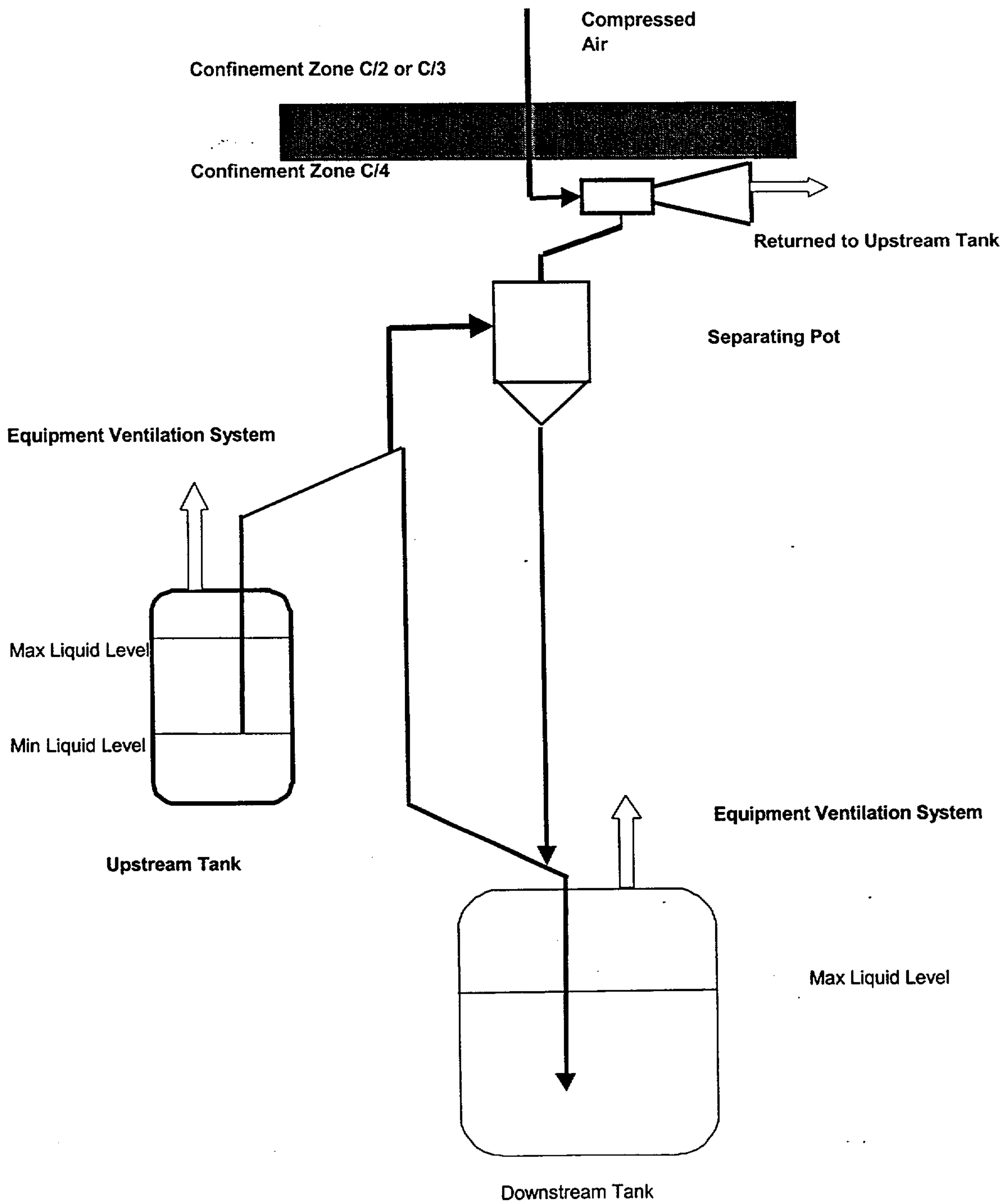
Component isolation in the event of an earthquake

MFFF process systems are shut down in the event that earthquake conditions are detected. This is achieved by the following:

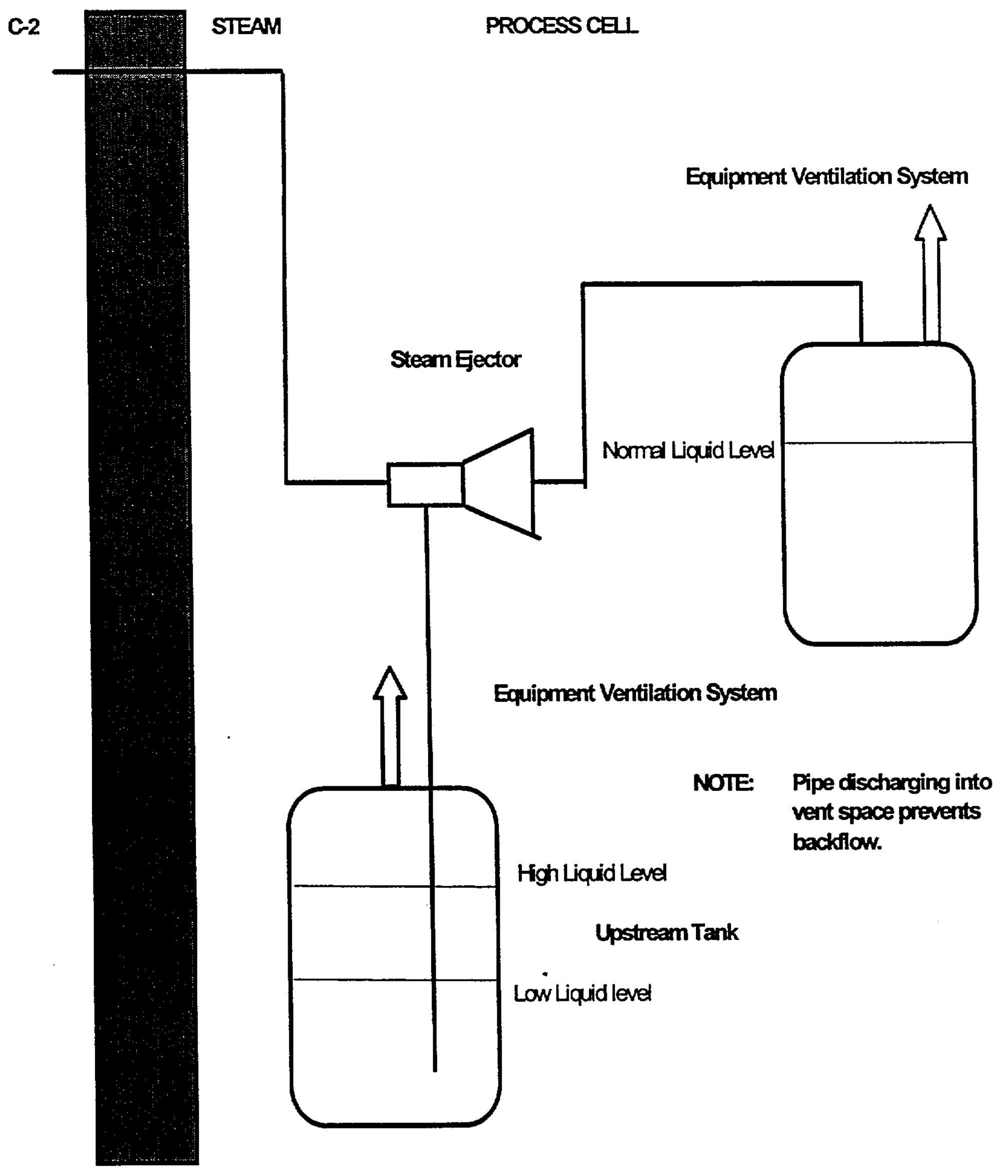
- Air and steam supplies that provide process fluid motive force are isolated by means of the redundant isolation valves described above.
- Process prime movers powered by normal electrical power are stopped. Those electrical loads requiring power for safe process shutdown are supplied with the emergency uninterrupted power.
- Fluid transport system components handling radioactive materials are designed for the design basis earthquake. In the event of system breach, liquids are collected at the bottom drip tray within the process cell or glove box and recycled through the waste treatment management units.

- Piping components handling the transfer of radiological process fluids outside of process cells and gloveboxes are double-wall jacketed construction. All piping components designated IROFS are designed to withstand design base earthquake conditions.

TYPICAL SCHEMATIC USING SIPHON AND AIR-JET LIFT FOR FLUID TRANSFER USING SEPARATION POT



TYPICAL SCHEME USING STEAM JET FOR FLUID TRANSFER



Action:

In the next update to the CAR, revise Section 11.8.7 as indicated above.

192. Section 11.8, pp. 11.8-1 thru 11.8-10

Discuss the use of traps in the fluid transport system where buildup of solids could occur. If they exist, describe where they are located and what measures will be taken to minimize the buildup of solids in the system.

Basis: Section 11.4.7.2.H of the SRP recommends that the use of traps where solids can buildup be avoided. This section applies to the specific design considerations for the fluid transport systems in general and to parts of the fluid transport system equipment identified as principle SSCs, in particular. No discussion of the use of traps where buildup of solids could occur is included in the application.

Response:

The following design information is provided:

The AP processes involve liquid processes except handling powder at the beginning and end of the aqueous polishing unit.

The process technology selected maintains the complete dissolution of powder in the aqueous polishing. The following discussion narrates the potential solid build-up corrective measures, in context with the processes involved.

Means are provided to minimize or eliminate the buildup of solids with the AP-liquid processes as follows:

- Process technology implemented does not involve suspension of the solid particles in liquid past the dissolution stage prior to precipitation.
- Undissolved particles are removed through the two-stage filtration in the dissolution unit.
- The liquid solutions used in the processes are not saturated solutions.
- Air spargers are provided as necessary to keep solutions well mixed.
- Appropriate process fluid velocities through the piping are maintained. Decontamination fluid is supplied to piping and equipment to remove any potential buildup.
- Piping layout is designed with an adequate slope, without sharp directional change, and without low point traps.
- Procedures for pipeline decontamination and de-clogging will be prepared for use in conjunction with the use of high pressure decontamination fluid to dissolve blockage.

Means are provided to minimize build-up of solids in the powder handling processes as follows:

- Process environment ensures that no moisture ingress can occur.
- The associated process equipment are stacked vertically. The shortest gravity feed chute and controlled vane volumetric feeders are used to feed the powder.
- The surface finish provides non-sticking tendencies.
- Provision of vibrators at the specific locations maintains the free fall gravity feed.

Action:

None

193. Section 11.8, pp. 11.8-1 thru 11.8-10

List parts of fluid transport systems for wet processing operations that do not meet the recommendation that wet processing operations involving gram quantities of plutonium or 50 micrograms or more of respirable plutonium be conducted in a glovebox.

Section 11.4.7.2.I of the SRP states that the application should describe the need for hoods, gloveboxes, and shielding. This recommendation applies to the specific design considerations for the fluid transport systems in general and to parts of the fluid transport system equipment identified as principle SSCs, in particular. No specific discussion was provided for fluid systems that involve gram quantities of plutonium or 50 micrograms or more of respirable plutonium, but are not conducted in a glovebox.

Response:

Components that handle radioactive materials in chemical solutions are fabricated from fully welded construction, and do not require routine operation maintenance, are located in the "Process Cell." The piping component that connects the process cell and glovebox equipment is fully welded double wall construction pipe. This process cell and welded equipment for liquid containing systems provide equivalent confinement to a glovebox. See CAR Section 11.4.1 for more information.

The fluid transport system components that handle radioactive materials in a chemical solution, and require access for routine operation maintenance are located in a glovebox.

Table 1 below provides a summary of the confinement principles as described in CAR Section 11.4.

Table 2 below provides a list of major equipment in process cells with greater than gram quantities of Pu.

Action:

None

Table 1
Summary of Confinement Principles for AP Systems

Physical state of radioactive products	Primary Confinement System	Secondary Confinement	
		1st barrier	2nd barrier
• In chemical solutions • Fully welded equipment (components that does not require operator intervention, and practically maintenance free)	• Full welded process equipment • Full welded pipe	Process cell + Welded Tray bottom for the process cell floor	Building
• In chemical solutions • Equipment that can be opened (components that require operator's routine intervention, and maintenance)	• Glovebox + • Drip tray	Process room	Building
• As powder canisters • As powder in process equipment	• Glovebox	Process room	Building

Table 2
List of Major Equipment in AP Process Cells Containing at Least Gram Quantities of Pu

Equipment Number			Description	Type of Equipment	Location
Unit	Type	Number			
KDB	TK	3000	Plutonium nitrate, Receiving Tank	Slab Tank	Process Cell
KDB	TK	4000	Plutonium nitrate, Receiving Tank	Slab Tank	Process Cell
KDB	TK	5000	Plutonium nitrate, Dilution and Sampling Tank	Slab Tank	Process Cell
KDB	TK	6000	Plutonium nitrate, Dilution and Sampling Tank	Slab Tank	Process Cell
KDB	TK	7000	Buffer Tank	Annular Tank	Process Cell
KPA	TK	1000	Plutonium nitrate, Feeding Tank	Annular Tank	Process Cell
KPA	PULS	2000	Extraction Column	Pulsed Column	Process Cell
KPA	PULS	2200	Scrubbing Column	Pulsed Column	Process Cell
KPA	PULS	3000	Pu stripping Column	Pulsed Column	Process Cell

Equipment Number			**Description**	**Type of Equipment**	**Location**
Unit	**Type**	**Number**			
KPA	PULS	3100	Diluent Washing Column	Pulsed Column	Process Cell
KPA	CLMN	6000	Oxidation Column	Column	Process Cell
KPA	CLMN	6500	Air stripping Column	Column	Process Cell
KPA	TK	7000	Pu reception Tank	Annular Tank	Process Cell
KPA	TK	8000	Pu Rework Tank	Slab Tank	Process Cell
KPA	TK	9000	Raffinates reception Tank	Annular Tank	Process Cell
KPA	TK	9100	Control Tank	Annular Tank	Process Cell
KPA	TK	9500	Recycling Tank	Annular Tank	Process Cell
KPB	TK	3000	Solvent regeneration waste Tank	Conventional Tank	Process Cell
KCA	TK	1000	Constitution Lot Tank	Annular tank	Process Cell
KCA	TK	2000	Constitution Lot Tank	Annular tank	Process Cell
KCD	TK	1000	Reception Tank	Annular Tank	Process Cell
KCD	TK	1500	Buffer Tank	Annular Tank	Process Cell
KCD	TK	2000	Feeding Tank	Annular Tank	Process Cell
KCD	EV	3000	Evaporator with Re-boiler	H/E, Evaporator	Process Cell
KCD	TK	4000	Concentrates reception Tank	Slab Tank	Process Cell
KCD	TK	4100	Concentrates control Tank	Slab Tank	Process Cell
KCD	TK	4200	Concentrate recycle Tank	Slab Tank	Process Cell
KPC	TK	1000	Feeding Tank	Conventional Tank	Process Cell
KPC	EV	2000	Evaporator with Re-boiler	H/E, Evaporator	Process Cell
KPC	TK	3000	Concentrates Tank	Conventional Tank	Process Cell

Equipment Number			**Description**	**Type of Equipment**	**Location**
Unit	**Type**	**Number**			
KPF	TK	1000	Re-circulation Tank	Conventional Tank	Process Cell
Main Process Piping for all above units			Double wall piping carrying process fluid with dissolved plutonium compounds	Double pipe carrying plutonium compound in liquid	Process Cell

194. Section 11.8, pp. 11.8-1 thru 11.8-10

Clarify where in the application decontamination characteristics are addressed.

Section 11.4.7.2.J of the SRP states that the application should demonstrate that surface finishes in the work areas are of materials that have satisfactory decontamination characteristics for their particular application. The fluid transport system section does not address decontamination characteristics of the equipment.

Response:

CAR Section 11.9.3.12 describes the decontamination system, which supplies decontamination fluid to fluid transport system components for decontamination. All fluid transport system components handling radioactive fluids are constructed of corrosion resistant materials to facilitate decontamination.

See the responses to Questions 188 and 189 for additional information concerning dust control and decontamination for material handling equipment.

Action:

None

195. Section 11.8.6, pp. 11.8-5

Clarify the design bases for non-principal SSCs and any impact these might have upon principal SSCs/IROFSs

Section 8.3 of the SRP states, "Information contained in the application should be of sufficient quality and detail to allow for an independent review, assessment, and verification by the reviewers. Some information may be referenced to other sections of the application, or incorporated by reference, provided that these references are clear, specific, and essentially complete." SRP Section 8.4.3.1 states that an application would be acceptable if it addresses the baseline design criteria for chemical safety and includes information on the chemicals, process, equipment, inventories, ranges, and limits. At the construction permit stage, this would be expected to include design bases and values for these items, with sufficient system description to allow verification of the design bases and values. Sections 8.4.3.5 B, C, D, and F recommend that design bases, process safety features, and IROFS be included in the application. Section 11.8.6, "Design Basis for Non-Principal SSCs," is simply a reference to Table 11.8-1. The section does not link specific codes and standards to specific SSCs and no design bases/values are provided. In addition, the distinction between non-safety SSCs and IROFSs is not clear. It is not clear how the linkage to an IROFS is addressed. More information is needed before a safety determination can be made.

Response:

The design ensures that principal SSCs are not adversely impacted by non-principal SSCs. The engineering design bases for non-IROFS fluid transport components (piping and welded equipment) are derived from the standard engineering practices and national codes as listed in CAR Table 11.8-1.

Principal SSCs are identified in CAR Chapter 5. IROFS will be identified during final design. Non-principal SSCs will contain double isolation valves and backflow prevention IROFS as described in the response to Question 196. Additionally, SSCs will be evaluated for potential interaction between non-principal SSCs and principal SSCs.

Action:

Update CAR Section 11.8.6.

196. Section 11.9, General

Provide information on the chemical double isolation valves and backflow prevention.

Section 8.3 of the SRP states, "Information contained in the application should be of sufficient quality and detail to allow for an independent review, assessment, and verification by the reviewers. Some information may be referenced to other sections of the application, or incorporated by reference, provided that these references are clear, specific, and essentially complete." SRP Section 8.4.3.1 states that an application would be acceptable if it addresses the baseline design criteria for chemical safety and includes information on the chemicals, process, equipment, inventories, ranges, and limits. At the construction permit stage, this would be expected to include design bases and values for these items, with sufficient system description to allow verification of the design bases and values. Sections 8.4.3.5 B, C, D, and F recommend that design bases, process safety features, and IROFS be included in the application.

In Section 11.9, double isolation valves are mentioned for many of the reagent systems, such as for hydrogen and nitric acid. Methods of actuation are not discussed. These valves would be activated by a seismic sensor system, which is not described further and no action limit is identified. Section 11.9.5.1 on page 11.9-51 is entitled, "Isolation Valves" in Section 11.9.5 entitled, "Design Basis for Principal SSCs." No design basis functions and values are identified for specific or general systems. Activation by other control systems in response to other stimuli/measurements (e.g., leak detectors) is not mentioned. In addition, breakpots are mentioned for some streams, but no further information could be found in the application. The description of these items implies some safety significance, but such significance is not identified in the application. However, at the public meeting of April 25, 2001, DCS stated the double isolation valves are principal SSCs/IROFSs. Sufficient information is not included in the report to address any potential hazards and safety functions associated with these SSCs. Design basis information and values, corrosion effect information, and an adequate system description are needed to assess the associated hazards and appropriateness of these valves and backflow preventers, and safety functions. For example, we would anticipate design basis information related to PFOD/reliability, leakage, aging/longevity requirements, activation methods/limits, IROFS/principal SSC status etc.

Response:

The principal SSCs for the fluid systems in CAR Section 11.9 include redundant isolation valves (IROFS) for each gas, utility, and reagent penetration into the BMF. These valves are provided to maintain confinement and to prevent uncontrolled discharge of the fluid into the BMF subsequent to a seismic event. These valves are not designed to prevent backflow. See the response to Question 191 for a discussion of backflow prevention.

Each isolation valve is independent and is located in a separate fire zone within the BMF area. A seismic sensor will send a signal directly to the pneumatic operator of the isolation valve (i.e., hard-wired) to vent air (valves fail to the closed position on loss of air). Closure of these valves by other stimuli or measurements is currently under study. The valves use power to open and fail in the closed position on loss of power. Position indicators (OPEN/CLOSE) will be provided in the Process and Utility Control Room and the Emergency Control Room to monitor performance.

Action:

None

197. <u>Section 11.9, pp. 11.9-1 thru 11.9-116</u>

Regarding the process chilled water system, describe how in-leakage of contaminated coolant from intermediate heat exchangers would be detected. If no means of detection is provided, provide the basis for this design configuration.

Section 11.4.4.2.F of the SRP states that the application should describe that capacity and capability for detecting leaks and cross-contamination. The application does not provide specific information as to the detection of contaminated coolant.

Response:

The Process Chilled Water (CHP) System is described in CAR Section 11.9.1.2.2. The primary means of detecting contaminated fluid in-leakage from the process systems into the CHP internal cooling loops will be by radiation detection in a continuous bypass flowpath in the common chilled water return line of each internal cooling loop. The chilled water return lines of each internal cooling loop will be continuously monitored with radiation alarms in the main control room.

Action:

Update the CAR to reflect the above information.

198. <u>Section 11.9, pp. 11.9-1 thru 11.9-116</u>

Regarding the process condensate system and the plant water system and other similar systems, describe the potential for chemical/radiological contamination of piping and components. In the event of an isolation, describe what would prevent potentially contaminated water from migrating or back flowing to other equipment, the Savannah River Site, or the MOX MFFF drinking water supplies.

Section 11.4.4.2.F of the SRP states that the application should describe that capacity and capability for detecting leaks and cross-contamination in cooling water systems. The application does not provide specific information as to the detection of contaminated water.

Response:

The primary condensate system can become contaminated only if the steam system is contaminated. A principle of the primary steam system is to have two physical boundaries between the primary steam system and potentially contaminated material. Primary steam is used to produce secondary steam and hot water, which in turn is used to heat potentially contaminated fluid. In these heat exchangers, the primary steam is at a higher pressure than the secondary steam and hot water. Therefore, primary steam would leak into the secondary steam or hot water in case of a tube rupture or other upset condition. There would not be any back flow into the primary steam system.

Primary steam is also used in steam jets. The only condensate collected in this area is from a separation pot upstream of the steam jets and a trap at the end of the steam header. The steam jets are used to transfer liquid from one tank to another. To protect from back flow and steam system contamination, the discharge tanks of the steam jets are at atmospheric pressure and the high points of the discharge lines are several feet below the steam inlet pipes in the active cell. Any back flow would enter the discharge tanks, not the steam system piping. Also, the steam jets are tied into the decontamination system so that the piping can be decontaminated periodically.

The secondary steam/condensate systems are a closed loop. The secondary condensate system can only be contaminated from the secondary steam system. Secondary steam is used to heat potentially contaminated fluid. The heating is done within a heat exchanger to create a physical boundary between the steam system and the process. Also, the secondary steam is at higher pressure than the fluid being heated. A system upset would cause the secondary steam to leak into the potentially contaminated fluid. The secondary condensate system is equipped with a radiation monitor as described by the response to Question197. The condensate tank has level instruments that detect level changes due to a system leak or in-leakage from the process or demineralized water system.

Heat exchangers are used as physical boundaries between the process and the hot water system. The hot water system is also equipped with a radiation monitor to detect any in-leakage of contaminated fluid. The hot water system operates at a higher pressure than the process fluids being heated to prevent in-leakage.

Both plant water and demineralized water are consumed by systems they supply. Since there is no recycling, there is not a risk of contaminating other systems. To prevent back flow, there is a check valve for each take-off from the plant water and demineralized water system headers. The plant water system has a back flow preventer installed in-line between the Savannah River Site and the MFFF. The demineralized water system has an atmospheric storage tank and an atmospheric buffer tank that act as pressure breaks in the system. These tanks along with a check valve installed at the MFFF boundary prevent back flow back to the Savannah River Site.

Prevention of contamination of the chilled water system is described in the response to Question 197.

There are no interfaces between the MFFF drinking water supply with any of the utilities.

Action:

None

199. Section 11.9, pp. 11.9-1 thru 11.9-116

Regarding the Emergency Diesel Generator (EDG) Fuel Oil System, explain if the exhaust system silencer/piping is an industry "standard design" rated for indoor use. Describe the industry standards. Describe the design basis criteria that the exhaust system meet to ensure the impact on operations or maintenance is minimal during EDG operation. Describe filtration of the diesel fuel oil. Describe how that is accomplished. Describe the criteria for the filters that will be used.

Standard Review Plan 11.4.2.2.C recommends, among other things, that the independent onsite power sources be designed to have no single failure vulnerability. Excessive noise and heat can be. Extreme noise in the EDG rooms could lead to operator fatigue and become a single failure vulnerability. The criteria and description of the industry standards and ratings for the EDG exhaust systems was not provided.

Response:

The Emergency Diesel Generator Fuel Oil Storage System (EGF) has been defined to include the fuel oil storage and transfer components and will exclude the diesel engine exhaust components. The diesel engine exhaust will be a component of the generator set that is included in the Emergency AC Power System (CAR Section 11.5.7.1) as a vendor provided packaged unit.

As stated in MFFF CAR Section 11.5.7.1, "...the Emergency Diesel Generator sets will be designed and qualified in accordance with IEEE Std 387 (1995)," which includes the engine exhaust. The engine exhaust will be provided as part of the generator set vendor package and will conform to NFPA-37 (1998) and NFPA-110 (1999). The function of the engine exhaust is to collect and remove exhaust as quickly and silently as possible. The primary design consideration is to minimize engine cylinder backpressure since exhaust gas restrictions can cause loss of engine performance and increase exhaust gas temperatures.

Some operator occupation of the generator set compartment may be necessary during engine operation but is not expected to be extensive since the EDG Control Panel, switchgear and motor control centers are located in the Switchgear Rooms. The engine exhaust system will be equipped with a silencer capable of noise attenuation to acceptable OSHA levels for personnel hearing protection in an industrial environment. In addition, the generator set is located in a separate, dedicated compartment of the Emergency Diesel Generator Building.

Heat generated by the exhaust system will be routed from the exhaust manifold into the compartment overhead (and eventually outside) by the exhaust piping and will be provided with heat shields at potentially accessible areas. Primary heat removal from the EDG building will be provided by the Emergency Diesel Generator Building HVAC System (HVD) as described in CAR Section 11.4.3.

Since the generator set is located in a separate, dedicated compartment with limited operator occupation during engine operation, outside air ventilation is provided to this area, and the inlet source is determined by engine operation. When the engine is not operating, roof ventilators controlled by local thermostats and interlocked with the diesel provide outside air ventilation. Upon engine start, the roof ventilators are de-energized and dampers (also interlocked with the diesel) open to provide a flow path for combustion and cooling air for the diesel. During engine operation, outside air is pulled into the generator room by the engine air intake system and by the engine-driven radiator fan. After passing through the radiator, the air is discharged to the back to the outside environment.

Fuel Oil Filtration

The MFFF Emergency Diesel Fuel Oil Storage System (EGF) has been designed to comply with ANSI / ANS 59-51-1997. The current configuration of the EGF System consists of two independent sub-systems, each capable of fuel receipt, long-term storage, and the ability to transfer an adequate supply of fuel oil to support its associated Emergency Diesel Generator operating at 100% load for seven days. Each sub-system consists of a main storage tank (located in an underground vault), a transfer system, an immediate use day tank, and a fuel purification system.

Fuel filtration and purification will be performed in five separate locations: (1) on receipt of new fuel from the remote fill station, (2) at the transfer pump suction, (3) in a by-pass flow purification system, (4) on delivery to the engine between the day tank and engine, and (5) at the engine itself. The fuel filter on the engine is considered as a component of the generator set and is not included in the EGF System.

The main storage tank fill line from the remote fill station will contain a multi-element, locally differential pressure instrumented (PDIs) inlet filter rated 2 μ to filter new fuel on receipt. The criteria used for this filter and its rating is to prevent coagulated fuel and/or particulate contaminants from entering the storage tank assuming a low-pressure flow of 80-100 gpm.

The transfer system includes the transfer piping (supply and return) between the main storage tank and the immediate use day tank. Motive force will be provided by a rotary screw positive displacement transfer pump with a differential pressure instrumented (PDIS), switchable dual-basket suction strainer with automatic transfer valve and will have a stainless steel mesh rating for 100% particulate removal at 45 μ and 98% particulate removal at 17 μ. The criteria used to size and rate of the transfer pump suction strainer is to prevent abrasive particulates from entering (and eventually damaging) the transfer pump based design flowrate and on pump manufacturer recommendations for pump running clearances. The suction strainer mesh rating for a typical rotary screw positive transfer pump is approximately 100 mesh (165 μ). The 45 μ strainer chosen is to ensure adequate protection for the close running tolerances of a typical rotary screw positive displacement pump. The design flowrate for the EGF System transfer pump (transfer fuel from the main storage tank to the immediate use day tank) is 25 gpm.

The immediate use day tank includes an engine supply line with differential pressure instrumented (PDIS), switchable dual-element basket strainer with automatic transfer valve. The filter media will be stainless steel mesh with an estimated rating at 100% particulate removal at 18 μ and 98% particulate removal at 5 μ. The fuel pump on the engine and not the transfer pump on the EGF System provide motive force. The criteria used to size and rate the engine supply strainer is to prevent overloading of the engine mounted fuel filter at the fuel inlet flowrate. The rating of a typical engine mounted fuel filter is approximately 5 μ based on engine requirements and will be supplied by the engine vendor as a component of the generator set. Typical supply flowrate is approximately 330 gph with approximately 72 gph used for combustion at 100% load and 258 gph returned to the Day Tank. These values are considered typical for this size EDG.

The purification system is a self-contained vendor package, which contains particulate filters and water-removal equipment and is connected to the transfer system supply and return lines. The Transfer Pump will provide the motive force to the purification skid with the purified fuel routed back to the Main Storage Tank. Periodic recirculation and purification of the EGF System will be a routine activity to assist in maintaining the diesel fuel in good condition. During recirculation, a portion (approximately 15 to 20 gpm) of the 25 gpm transfer flow between the Main Storage Tank and Day Tank will by-pass the Day Tank and be routed through the purification package. The remainder of the recirculation flow (approximately 5 to 10 gpm) will be routed to the Day Tank and will ensure that adequate supply can be delivered as make-up to the Day Tank in the event of an engine start during recirculation. Fuel consumption rate @ 100% load = 72.2 gph = 1.2 gpm. Day Tank overflow is returned to the Main Storage Tank. Recirculation for one shift (12 hours) will turnover, filter and purify the entire volume of the Main Storage and Day Tanks at least one time. Particulate filtration will be approximately 1 to 5 μ to remove abrasive particles that could damage the transfer pump and/or engine. Water removal equipment is typically coalescing filters to removal suspended water introduced into storage tanks by condensation from tank vents. After recirculation, all of the transfer flow will be routed to the Day Tank.

Action:

In the next update of the CAR, revisions to Section 11.9.1.7.2 and Figure 11.9-2 will be provided to reflect the above response.

200. Section 11.9, pp. 11.9-1 thru 11.9-116

Regarding the Instrument Air System, explain the basis for the 7-day emergency scavenging air supply. Describe the basis for the sizes of the 10-minute and 1-hour receivers/buffer tanks.

10 CFR Part 70.22(a)(7) requires the application for a license contains a description of equipment and facilities which will be used by the applicant to protect health and minimize danger to life or property. 10 CFR Part 70.61(e) requires that controls or systems needed to meet performance requirements be designated as an item relied upon for safety. Section 11.4.3.2.G of the SRP recommends that systems have capability to maintain functionality when subjected to natural phenomena as established in the ISA. The basis for the 7-day emergency scavenging air supply and the sizes of the 10-minute and 1-hour receiver/buffer tanks were not provided.

Response:

Seven days is considered a reasonable period for restoration of the normal bubbling air supply for use in vessel scavenging following failure of the instrument air system. The emergency scavenging air system provides air to prevent radiolysis-related hydrogen buildup following a loss of the normal air supply.

The receiver buffer tanks provide air to facilitate a normal process shutdown following loss of the instrument air system.

The instrument air system has been modified to eliminate the 10-minute buffer tanks. The one-hour capacity provides sufficient air for an orderly shutdown of process operations.

See the response for Question 122 for additional information on the emergency scavenging air supply system.

Action:

Update the CAR to reflect the above information.

201. <u>Section 11.9, pp. 11.9-1 thru 11.9-116</u>

Regarding the Instrument Air System, identify any parts or functions of the system that are part of or support the "glovebox pressure controls." The system description discusses aqueous polishing glovebox scavenging and supporting miscellaneous equipment, however Figure 11.9-10 shows interfaces with MOX processing gloveboxes. Define the term "miscellaneous equipment." Section 11.9.1.10.5 of the application, "System Interfaces," only lists the Service Air System and the Seismic Detectors as interfacing systems. The general description of gloveboxes in Section 11.4.7.1.5 does not list the Instrument Air System as an interface. Please clarify the functions and all interfaces of the Instrument Air System and clarify its safety function, if any, and whether any part of this system is a primary SSC or an item relied upon for safety. Provide the basis for the basis for your conclusions. Clarify the functions and interfaces of the scavenging air system.

10 CFR Part 70.22(a)(7) requires the application for a license contains a description of equipment and facilities which will be used by the applicant to protect health and minimize danger to life or property. The application does not clearly explain the interfaces and functions of the instrument air system.

Response:

<u>Regarding the Instrument Air System, identify any parts or functions of the system that are part of or support the "glovebox pressure controls."</u>

The Instrument Air System (IAS) described in CAR Section 11.9.1.10 does not provide or support "glovebox pressure controls" but rather it provides dry air to Decanning, Dissolution, Homogenization and Canning gloveboxes in the AP area and to the PuO_2 Receiving and Buffer Storage gloveboxes and the hydraulic presses glovebox bellows in the MP area during normal operation. The Instrument Air System interfaces with the Very High Depressurization System (VHD) and provides dry air for glovebox ventilation. The VHD system independently controls the glovebox pressure (see CAR Section 11.4.2.2 for description of the VHD control system).

<u>The system description discusses aqueous polishing glovebox scavenging and supporting miscellaneous equipment; however, Figure 11.9-10 shows interfaces with MOX processing gloveboxes. Define the term "miscellaneous equipment."</u>

Miscellaneous equipment refers to the air lift pumps used for vessel mixing and material transport and to the air ejectors used for vessel vapor space evacuation.

Bubbling air is used for level measurement in vessels. It also provides normal scavenging air to vessels containing compounds that undergo radiolysis to form hydrogen. If the normal bubbling air is lost, an Emergency Scavenging Air System is used as discussed in the response to Question 122. Although the Emergency Scavenging Air System is used to replace the normal scavenging air supply, it is not physically connected to the normal scavenging air supply (i.e., it has a separate nozzle to supply the vessel/tank).

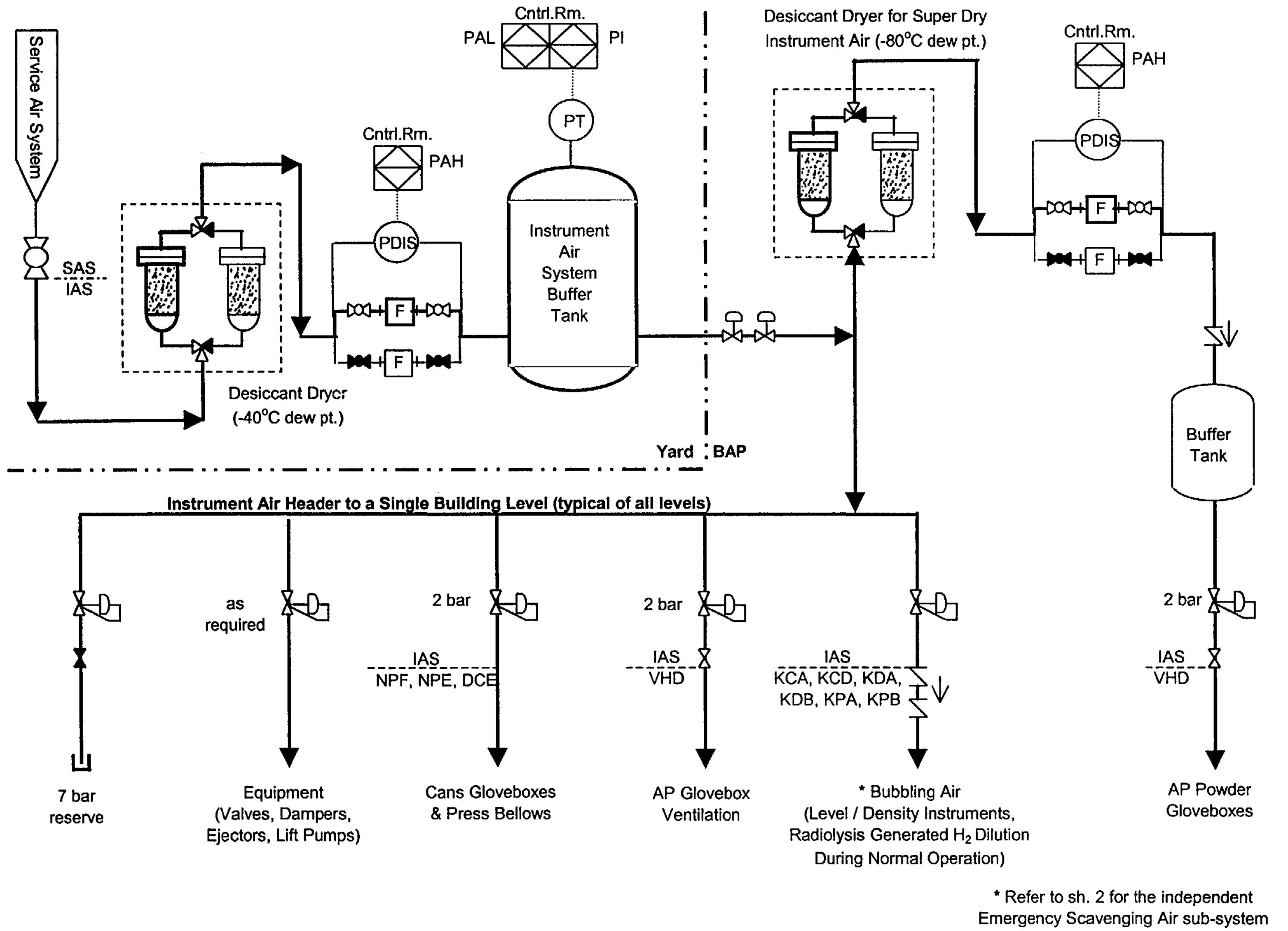
The equipment that will receive Emergency Scavenging Air during normal and emergency operations has been identified in the response to Question 122.

Section 11.9.1.10.5 of the application, "System Interfaces," only lists the Service Air System and the Seismic Detectors as interfacing systems. The general description of gloveboxes in Section 11.4.7.1.5 does not list the Instrument Air System as an interface.

The additional interfaces with the Instrument Air System are as follows:

- Very High Depressurization (VHD) Exhaust System: IAS provides instrument quality air for ventilation and cooling air for sixteen (16) AP and two (2) MP gloveboxes and the MP pelletizing press bellows.
- Very High Depressurization (VHD) Exhaust System: Super dry air (-80°C dew pt.) is used for ventilation and cooling of the AP powder and electrolyzer gloveboxes.
- The I&C system uses bubbling air in all AP process units to measure level and density.

Refer to attached sketch.


Service Air System
SAS
IAS
Desiccant Dryer
(-40°C dew pt.)
Cntrl.Rm.
PAH
PDIS
F
F
Cntrl.Rm.
PAL
PI
PT
Instrument Air System Buffer Tank
Yard
BAP
Desiccant Dryer for Super Dry Instrument Air (-80°C dew pt.)
Cntrl.Rm.
PAH
PDIS
F
F
Buffer Tank
Instrument Air Header to a Single Building Level (typical of all levels)
as required
2 bar
IAS
NPF, NPE, DCE
2 bar
IAS
VHD
IAS
KCA, KCD, KDA, KDB, KPA, KPB
2 bar
IAS
VHD
7 bar reserve
Equipment (Valves, Dampers, Ejectors, Lift Pumps)
Cans Gloveboxes & Press Bellows
AP Glovebox Ventilation
* Bubbling Air (Level / Density Instruments, Radiolysis Generated H2 Dilution During Normal Operation)
AP Powder Gloveboxes
* Refer to sh. 2 for the independent Emergency Scavenging Air sub-system

Please clarify the functions and all interfaces of the Instrument Air System and clarify its safety function, if any, and whether any part of this system is a primary SSC or an item relied upon for safety. Provide the basis for your conclusions.

The functions of the Instrument Air System include, but are not limited to, the following:

Supply instrument quality air (as defined by ANSI/ISA-S7.0.01-1996, "Quality Standard for Instrument Air) or better for the following:

- Instrumentation, air-operated valves and HVAC dampers
- Ventilation and cooling air for gloveboxes and the pelletizing press bellows
- Normal bubbling / scavenging air for level measurement and hydrogen dilution during normal operation.
- Independent emergency scavenging air for plutonium vessels to prevent radiolysis-related hydrogen buildup following an earthquake, loss of normal instrument air, or loss of power.
- Super dry (-80°C dew pt.) process air for ventilation and cooling of the AP powder gloveboxes

The Emergency Scavenging Air System is the portion of the Instrument Air System that is identified as a principal SSC. The Emergency Scavenging Air System supplies air to vessels containing plutonium to prevent radiolysis-related hydrogen buildup following an seismic event, loss of normal instrument air, or loss of power. See the response to Question 122.

Clarify the functions and interfaces of the scavenging air system.

The "Scavenging Air System" is an independent subsystem of the Instrument Air System. The term "scavenging air" as used here is for air performing a "purge" or "dilution" of any radiolysis generated hydrogen in a vessel vapor space and not a chemical reaction (such as excess hydrogen scavenging or combining with free oxygen). During normal operation, the Instrument Air System (-40°C dew point) provides bubbling air to level instrumentation in Process vessels (including those that contain Pu). During normal operation, this level instrumentation bubbling air also functions as the scavenging air for each vessel. During an emergency or loss of normal Instrument Air, the Emergency Scavenging Air subsystem portion of the Instrument Air System fulfills the scavenging air function to all vessels containing Pu that are undergoing radiolysis to form hydrogen. This subsystem is completely independent of the normal bubbling air for the Instrument Air System and is described fully in the response to Question 122.

Action:

Revise CAR Section 11.9.1.10 to include applicable portions of response to this question and Question122, including enclosed figures.

202. Section 11.9, pp. 11.9-1 thru 11.9-116

Regarding the Radiation Monitoring Vacuum System (RMVS), describe how a failure in the RMVS be detected. Describe any alarms and where they would display if provided. Clarify if this system is relied on by the training program as an indicator to take emergency actions. Provide justification why this system should not be classified as a principle SSC.

10 CFR Part 70.22(a)(7) requires the application for a license contains a description of equipment and facilities which will be used by the applicant to protect health and minimize danger to life or property. The application does not provide sufficient information for a reviewer to find that the equipment is adequate to protect public health and safety and minimize danger to life and property.

Response:

Leaks within the Radiation Monitoring Vacuum System (VRM) will be identified by the continuous air monitors (CAMs) that are attached to the VRM piping distribution system. A CAM triggers an alarm in the Polishing & Utilities Control Room following a total loss or lack of adequate vacuum. The triggering of many alarms would indicate the loss of vacuum to a header, or to the total vacuum system. In addition, vacuum pressure monitors will be located throughout the major branches of VRM to provide early indication of reduced vacuum, and possible vacuum loss or system leakage. Parallel liquid ring vacuum pumps, each designed for the system capacity, will be used to ensure continuity of vacuum during maintenance.

Neither CAMs, nor the Radiation Monitoring Vacuum System that supports the CAMs, are relied on for safety. These systems are not credited in the CAR Chapter 5 (Safety Assessment) for preventing or mitigating an accident to meet the performance requirements of 10 CFR 70.61 for workers and public. Therefore, neither CAMs nor the VRM are classified as a principal SSC.

The radiation monitoring system is not required to meet the performance requirements of 10 CFR 70.61, and therefore are not required to protect public health and safety or to minimize danger to life and property.

Action:

None

203. Section 11.9, pp. 11.9-1 thru 11.9-116

Regarding the Nitric Acid System and all other applicable reagent systems in the MFFF, the descriptions of the tanks generally contain actions/contingencies for low tank level. Describe the design basis to protect against high tank level or overfill. Clarify how the release of tank contents from an overfill (of the nitric acid or nitrogen oxide tanks, for example) effect the adjacent MFFF. Describe the features that prevent escaping tank contents (liquids/gasses/vapors) from affecting workers in the MFFF or principle SSCs on the site.

10 CFR Part 70.22(a)(7) requires the application for a license contains a description of equipment and facilities which will be used by the applicant to protect health and minimize danger to life or property. No description of provisions or protection from tank overfill/release was given in the application. Supporting equipment must not interfere with the use or operation of IROFS.

Response:

As stated in Section 5.5.2.10, workers mainly perform a monitoring function during emergency conditions. To ensure that workers can perform this function, the Emergency Control Room Air Conditioning system is designated as a principal SSC. Its function is to ensure habitable conditions for workers in the emergency control rooms are maintained. Upon completion of the chemical consequence analysis, measures will be provided, if necessary, to ensure that emergency control room workers are protected from potential chemical releases.

Tank level controls for the reagent liquid systems are not principal SSCs and consequently were not included in Sections 11.6 and 11.9 of the CAR. For this example, however, downstream tanks are equipped with high level switches (via a transmitter to the system computer) that automatically shutdown the upstream transfer pump to avoid overflow in the tank. Even if overflow were to occur, retention sumps or drip pans would collect the overflow and have no effect on the operation of the MFFF.

Similarly, low level switches in upstream tanks are provided to shutdown the immediate downstream transfer pump to prevent starving the transfer pump and possibly causing overheating of the liquid.

Noxious fumes (e.g., NO, nitric acid, and TBP) are removed from equipment via vent lines and appropriately placed hoods to prevent worker exposure. Further, nitric acid and nitric oxide exhausts are treated in simple wet scrubbers before discharge to the atmosphere.

See the response to Question 111 for addition information on tank controls. See the response to Question 54 for a discussion of chemical hazards.

Action:

None

204. Section 11.9, General

Discuss the potential hazards associated with gas cylinders and any needed safety controls.

Section 8.3 of the SRP states, "Information contained in the application should be of sufficient quality and detail to allow for an independent review, assessment, and verification by the reviewers. Some information may be referenced to other sections of the application, or incorporated by reference, provided that these references are clear, specific, and essentially complete."

Section 11.9 indicates that high pressure gases and gas cylinders will be used within the facility. Little additional information is provided in the application. A compressed gas industry standard (CGA P-1) is mentioned on page 11.9-50. However, over a 10-20 year operating period for the facility, compressed gas cylinder incidents might be anticipated events if the usage rate is significant or have an unlikely likelihood if the usage rate is small (like a laboratory). Before a safety determination can be made, more information is needed to assess potential hazards such as regulator failures, dropped cylinders, and cylinder missiles; their potential impact upon the safe handling of any licensed radioactive materials; design bases and probabilities; and any safety controls.

Response:

CAR Chapter 5 identifies pressure vessel controls as a principal SSC whose safety function is to ensure that primary confinement and other principal SSCs are protected from potential pressure vessel failures. Most gas cylinders that are located in the same area as principal SSCs will be structurally prevented from causing an impact. Specific IROFS will be identified in the ISA.

Standard high volume compressed gas trailers are used to supply gaseous argon, helium, hydrogen, and emergency argon/hydrogen backup gases to various MFFF users. Primary nitrogen will be generated onsite; however, a liquid nitrogen supply tank is required to complement the nitrogen generating system and to supply nitrogen in event of failure of the primary generating system. The use of liquid nitrogen within the BMP will be eliminated by use of dedicated local chiller units for the radiation detectors in the 3013 can receiving area; these units can provide liquid nitrogen temperatures without actual use of liquid nitrogen.

Compressed gas storage cylinders will be used to supply emergency breathing air, argon-methane (P-10 gas) for personnel monitoring, emergency scavenging air for AP area, and process oxygen for the calciner in the AP area. With the exception of emergency breathing air and emergency scavenging air that are located within the BMP, all gases will be isolated with redundant seismic isolation valves just as with the liquid utilities and reagents (principal SSCs).

The compressed gas cylinders are subject to the regulations of the U.S. Department of Transportation (DOT) as found in 49 CFR Parts 100-199 and are constructed per the ASTM Boiler and Pressure Vessel Code. They are also tested and inspected per Compressed Gas Association (CGA) standards C-1 through C-15 and E-1 through E-6.

Nitrous oxide cylinders are not equipped with pressure relief devices. Authorized shipping containers and specifications are found in 49 CFR 173.336.

Cylinder connections will be industry standards as found CGA V-1 (1987):

CGA Series	GAS	RATING	STANDARD	ADDED 1987
G-7/G-7.1	Air	3000 psig	346	-
G-11.1	Argon	3000 psig	580	-
	Argon	Cryogenic	295	-
G-9.1	Helium	3000	580 (Threaded)	-
	Helium	Cryogenic	792	-
G-5/G-5.3	Hydrogen	3000 psig	350	-
	Hydrogen	Cryogenic	795	-
G-10.1	Nitrogen	3000 psig	580	-
	Nitrogen	Cryogenic	295	-
G-8.1/G-8.2	Nitrogen Dioxide (Dinitrogen Tetroxide)		-	660
G-4, G-4.1 & G-4.5	Oxygen	3000 psig	540	-
	Oxygen	Cryogenic	440	-

Outside of process usage, the other application that requires use of high-pressure cylinders is laboratory usage. Nearly all gases have localized laboratory applications. Laboratory usage of high-pressure cylinders is small.

Normal precautions related to the transportation, installation, and use of high-pressure cylinders will be followed. For example, high-pressure cylinders will be kept secured and capped while being transported. They will be transported or secured only in the vertical position. While in use, they will be secured to walls using metal brackets. However, detailed procedures for handling and storage of high-pressure cylinders will only be developed as part of the detailed system description documents. Recommendations of CGA publication P-1 Safe Handling of Compressed Gases in Containers will be followed.

Action:

None

205. Section 11.9, pp. 11.9-1 thru 11.9-115

Provide design basis information and commitments for the "Fluid Systems" presented in Section 11.9.

Section 8.3 of the SRP states, "Information contained in the application should be of sufficient quality and detail to allow for an independent review, assessment, and verification by the reviewers. Some information may be referenced to other sections of the application, or incorporated by reference, provided that these references are clear, specific, and essentially complete." SRP Section 8.4.3.1 states that an application would be acceptable if it addresses the baseline design criteria for chemical safety and includes information on the chemicals, process, equipment, inventories, ranges, and limits. At the construction permit stage, this would be expected to include design bases and values for these items, with sufficient system description to allow verification of the design bases and values. Sections 8.4.3.5 B, C, D, and F recommend that design bases, process safety features, and IROFS be included in the application.

Section 11.9 describes several fluid and reagent systems. Some design basis information is included, but it is generally inadequate to assess the potential safety of the proposed approach. The NRC would anticipate a clear communication of the system description, appropriate design bases and values, ranges, control information, needed reliabilities, and identification of any IROFSs. The NRC would expect any commitments to be clearly identified and stated, and, if the control concepts in Section 11.9.2.x.4 represent commitments, then they should be stated as such. In addition, these systems appear to rely heavily on operator actions and interactions, and, thus, human reliabilities should be included in the description and analyses.

Response:

In Section 11.9.5, the following principal SSCs were identified for "Fluid Systems":

1. Section 11.9.5.1 – Isolation of systems penetrating the BMF by use of automatically actuated, seismically qualified, redundant isolation valves on all fluid system penetrations. See the response to Question 196 for additional design detail.

2. Section 11.9.5.2 - The Emergency Diesel Fuel system for the Emergency Generator system. See the response to Question 199 for additional design detail.

3. Section 11.9.5.3 – Scavenging air for vessels and equipment in the BAP process areas that produce hydrogen by radiolysis and that could reach the LEL of hydrogen in air (4%) in seven days. The emergency scavenging air supply will ensure that the hydrogen concentration does not exceed 25% of the LEL value. See the response to Question 200 for additional design detail.

A principal SSC associated with the argon/hydrogen system and located at the sintering furnaces has been identified in the CAR. See the response to Question 124 for design basis information.

Action:

None

206. Section 11.9, pp. 11.9-1 thru 11.9-115

Describe the integration of the different Fluid Systems presented in Section 11.9.

Section 8.3 of the SRP states, "Information contained in the application should be of sufficient quality and detail to allow for an independent review, assessment, and verification by the reviewers. Some information may be referenced to other sections of the application, or incorporated by reference, provided that these references are clear, specific, and essentially complete." SRP Section 8.4.3.1 states that an application would be acceptable if it addresses the baseline design criteria for chemical safety and includes information on the chemicals, process, equipment, inventories, ranges, and limits. At the construction permit stage, this would be expected to include design bases and values for these items, with sufficient system description to allow verification of the design bases and values. Sections 8.4.3.5 B, C, D, and F recommend that design bases, process safety features, and IROFS be included in the application.

Section 11.9 provides a limited description of the fluid systems at the proposed facility, including chemical reagent systems. It is not clear how the different systems are integrated and interlocked to avoid potentially hazardous situations. A clearer system description with the identification of design bases and controls is needed before a safety determination can be made. For example, oxidizers and reductants could be handled in the same area, at concentrations well above those used in the process. The wrong material could be inadvertently added to the wrong vessel or line. Other incompatibilities might be possible. Some of the reagents can also volatilize and affect operators, potentially affecting the safe handling of radioactive materials. During operations at the proposed facility, numerous interactions would occur between operating personnel, the control room, the control system, and local controls. The operators may even be called upon to activate safety systems or undertake safety-type actions (e.g., avoid overfilling of tanks and vessels. It is not clear how these operator interfaces would function and what indicators are available for these operators, what are the required response times, reliabilities etc. The NRC would expect this type of information to be included in the application.

Response:

Each reagent fluid system is transferred from the preparation area in the reagents building or within the AP area to designated equipment and/or process units via a dedicated pipeline. Independent testing and sampling will also confirm that the reagent concentrations are correct before they can be transferred by the control room operator to the process areas.

Interaction between different chemicals is avoided by providing separate areas for storage and separate areas for preparation. The nitric oxide, solvent, and hydrazine/HAN areas are placed into separate rooms for full isolation.

A local operator will prepare all reagent solutions and gas. Samples will be manually taken by the local operators using established procedures and then placed at the lab for analysis. Results will be posted to the local operator but transfer to any downstream tank or system can only be independently initiated by the control room operator on the basis of correct reagent composition.

Hydraulic seals as described in the response to Question 190 provide isolation of liquid reagents from tanks and vessels containing radioactive materials.

See the response to Question 54 for a discussion of worker actions.

Specific IROFS to ensure that inadvertent chemical reactions do not occur will be identified in the ISA.

Action:

None

207. Section 11.9.2.1, pp. 11.9-23 thru 11.9-25

Provide additional design basis information on the nitrogen system.

Section 8.3 of the SRP states, "Information contained in the application should be of sufficient quality and detail to allow for an independent review, assessment, and verification by the reviewers. Some information may be referenced to other sections of the application, or incorporated by reference, provided that these references are clear, specific, and essentially complete." SRP Section 8.4.3.1 states that an application would be acceptable if it addresses the baseline design criteria for chemical safety and includes information on the chemicals, process, equipment, inventories, ranges, and limits. At the construction permit stage, this would be expected to include design bases and values for these items, with sufficient system description to allow verification of the design bases and values. Sections 8.4.3.5 B, C, D, and F recommend that design bases, process safety features, and IROFS be included in the application.

Section 11.9.2.1 describes the nitrogen system. Five primary and several backup functions are listed - it would be helpful to have the safety significance of these functions identified. The "Description" and "Major Components" sections appear contradictory and need clarification; the first part implies cryogenic storage as a backup while the second implies cryogenic supply is the primary storage means. Pressures, temperatures, quantities, purity, monitoring devices, control sensors and element design bases, interfaces for backup functions, and principal SSCs/IROFSs are not identified. This information is needed in order to make a determination regarding adequate safety.

Response:

There are no safety functions provided by the nitrogen system with the exception of isolation and backflow prevention into the system. See the response to Question 196 for additional design detail.

The operational aspects associated with the nitrogen system are addressed below.

- Nitrogen is used for BMP glovebox ventilation.
- Nitrogen is used for scavenging in the sintering furnace airlock. When the Mo-boat comes out of the furnace, it is under an $Ar\text{-}H_2$ atmosphere. Nitrogen flow in the airlock scavenges the $Ar\text{-}H_2$ to ensure that $Ar\text{-}H_2$ is eliminated.
- The rear bearing of the calcination furnace is scavenged with nitrogen for containment purposes. Nitrogen is selected over extra dry air to avoid damage to graphite bearings.
- Hydrazine tanks and Hydroxylamine Nitrate tanks containing hydrazine are provided with a continuously vented nitrogen blanket. Details of the operations associated with the nitrogen blanket are covered in response to Question 125.

The nitrogen system consists of the primary gaseous nitrogen generating unit and a secondary liquid nitrogen backup unit:

1. The primary source of gaseous nitrogen uses permeation based gas phase separation technology that produces gaseous nitrogen at the required rate and pressure. Ambient air is compressed and separated into nitrogen and an oxygen rich component that is discarded. This technology does not require cryogenic separation. Various vendors can provide nitrogen generation system as a leased, complete skid-mounted package that will be supplied and maintained by the vendor.

2. The secondary backup source for gaseous nitrogen production will be provided by an on-site liquid nitrogen storage tank with an ambient temperature vaporizer. Nitrogen will be vaporized to provide gaseous nitrogen in the event of failure of the primary nitrogen system. The backup liquid nitrogen supply will be designed to provide at least two (2) days of gaseous nitrogen supply.

The operating parameters for the nitrogen system are

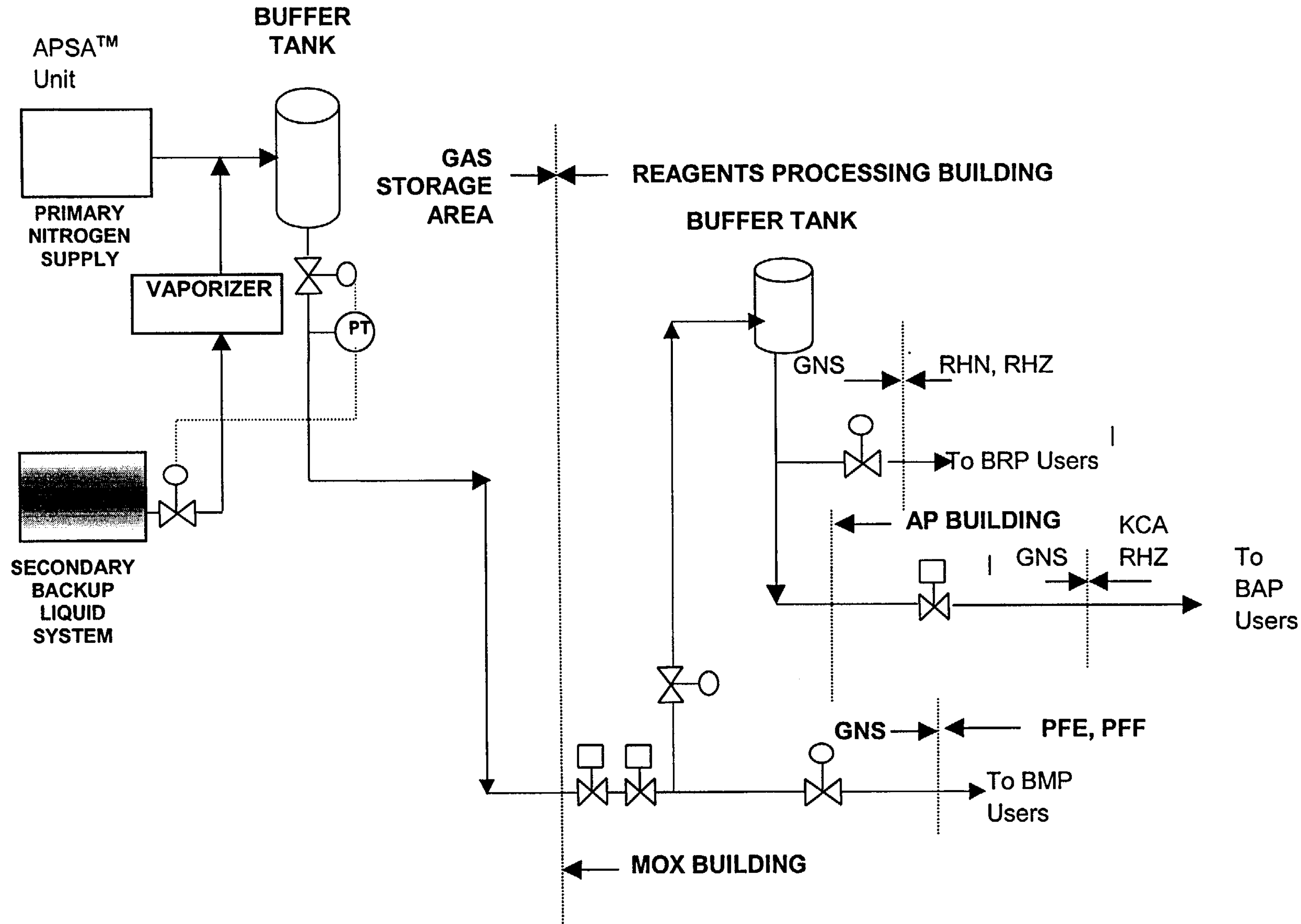
Temperature	Pressure, psig	Flow Rate, scfh
Ambient	30 - 100	17,500 – 19,800

The nitrogen system under consideration provides purity greater than 99.999%. The required impurity level for oxygen inside the glovebox is O_2 <2000 ppm so any industrial grade nitrogen supply is adequate. Normal industrial grade nitrogen supply meets 10 ppm or less impurity level in nitrogen and will be used.

The general principle for monitoring and control is the use of pressure regulation in the system using pressure transmitter and pressure control valve. Pressure monitoring is also used to transfer to the backup liquid supply if the primary gaseous nitrogen supply is lost. This control scheme has been added to the modified CAR sketch. However, the instrumentation details have not been developed sufficiently to respond to requests for monitoring devices, control sensors, etc.

Action:

Revise the CAR to include the modified sketch.


APSA™ Unit
PRIMARY NITROGEN SUPPLY
BUFFER TANK
VAPORIZER
PT
SECONDARY BACKUP LIQUID SYSTEM
GAS STORAGE AREA
REAGENTS PROCESSING BUILDING
BUFFER TANK
GNS
RHN, RHZ
To BRP Users
AP BUILDING
GNS
KCA RHZ
To BAP Users
GNS
PFE, PFF
To BMP Users
MOX BUILDING

208. Section 11.9.2.2, pp. 11.9-25 thru 11.9-27

Provide additional design basis and IROFS information on the argon/hydrogen system.

Section 8.3 of the SRP states, "Information contained in the application should be of sufficient quality and detail to allow for an independent review, assessment, and verification by the reviewers. Some information may be referenced to other sections of the application, or incorporated by reference, provided that these references are clear, specific, and essentially complete." SRP Section 8.4.3.1 states that an application would be acceptable if it addresses the baseline design criteria for chemical safety and includes information on the chemicals, process, equipment, inventories, ranges, and limits. At the construction permit stage, this would be expected to include design bases and values for these items, with sufficient system description to allow verification of the design bases and values. Sections 8.4.3.5 B, C, D, and F recommend that design bases, process safety features, and IROFS be included in the application.

Section 11.9.2.2 describes the argon/hydrogen system. Some pressure information is provided for hydrogen and the argon/hydrogen mixture; no pressure information is provided for the argon itself. No flow rates or quantities are provided. IROFSs are not identified. However, redundant hydrogen monitors, regulators, flow control valves, seismic detectors, and backup systems would imply safety-related functions for these SSCs. Reliabilities for these SSCs are not mentioned. Without this additional design basis and safety information, it is not possible to make a safety determination regarding the proposed facility.

Response:

Refer to the response to Question 124 for a description of the safety functions associated with this system. Additional principal SSCs include isolation of the system and backflow prevention. See the response to Question 196 for additional information.

The following is a description of the major system functions. Refer to CAR Section 11.9.2.2.1.

Action:

In the next update of the CAR, revise Section 11.9.2.2 to include this information.

209. Section 11.9.2.3, pp. 11.9-27 and 11.9-28

Provide additional design basis and IROFS information on the helium system.

Section 8.3 of the SRP states, "Information contained in the application should be of sufficient quality and detail to allow for an independent review, assessment, and verification by the reviewers. Some information may be referenced to other sections of the application, or incorporated by reference, provided that these references are clear, specific, and essentially complete." SRP Section 8.4.3.1 states that an application would be acceptable if it addresses the baseline design criteria for chemical safety and includes information on the chemicals, process, equipment, inventories, ranges, and limits. At the construction permit stage, this would be expected to include design bases and values for these items, with sufficient system description to allow verification of the design bases and values. Sections 8.4.3.5 B, C, D, and F recommend that design bases, process safety features, and IROFS be included in the application.

Section 11.9.2.3 describes the helium system. This system provides high pressure helium for rod pressurization and low pressure helium for welding, scavenging, and purging applications. Several components, such as the helium detectors, regulators, pressure switching system, and isolation valves imply a safety-related function, but IROFSs are not identified. Reliabilities are not mentioned. Without this additional design basis and safety information, it is not possible to make a safety determination regarding the proposed facility.

Response:

There are no safety functions provided by the helium system with the exception of isolation and backflow prevention into the system. See the response to Question 196 for additional design detail.

The pressure regulators, pressure switches, alarms, relief valves, and other isolation valves will be designed in accordance with CGA G-9 *(Helium)* and other industrial standards for tube trailers, valves, and piping.

High-pressure helium (363 psig) is used for pressuring the rods and low-pressure helium (44 psig) for rod welding as stated in the Construction Authorization Request. Some helium will be used in the laboratory from local cylinders; however, no other uses have been identified.

Refer to the response to Question 128 for confirmation of process parameters such as temperature, pressure, and flow for the helium system.

Action:

None

210. Section 11.9.2.4, pp. 11.9-28 and 11.9-29

Provide additional design basis information on the oxygen system.

Section 8.3 of the SRP states, "Information contained in the application should be of sufficient quality and detail to allow for an independent review, assessment, and verification by the reviewers. Some information may be referenced to other sections of the application, or incorporated by reference, provided that these references are clear, specific, and essentially complete." SRP Section 8.4.3.1 states that an application would be acceptable if it addresses the baseline design criteria for chemical safety and includes information on the chemicals, process, equipment, inventories, ranges, and limits. At the construction permit stage, this would be expected to include design bases and values for these items, with sufficient system description to allow verification of the design bases and values. Sections 8.4.3.5 B, C, D, and F recommend that design bases, process safety features, and IROFS be included in the application.

Section 11.9.2.4 describes the oxygen system. Some of the components, such as regulators, pressure monitors, switch-over systems, and the isolation valves, would appear to have safety-like functions, but IROFSs are not identified. Reliabilities are not identified. Without this information, it is not possible to make a safety determination regarding the proposed facility.

Response:

There are no safety functions provided by the oxygen system with the exception of isolation and backflow prevention into the system. See the response to Question 196 for additional design detail.

The pressure regulators, pressure switches, automatic switchover valve system, alarms, relief valves and other isolation valves are not IROFS and will be designed in accordance with Compressed Gas Association (CGA) G-4 *(Oxygen)* and other industrial standards for cylinders, valves and piping.

Oxygen is used in the calcination furnace in the KCA. The oxygen cylinders (2) will be located on the north end of the unloading dock at the BRP and will be routed through the BRP to the BAP.

Action:

None

211. Section 11.9.3.1, pp. 11.9-29 thru 11.9-32

Provide additional design basis and IROFS information on the nitric acid systems.

Section 8.3 of the SRP states, "Information contained in the application should be of sufficient quality and detail to allow for an independent review, assessment, and verification by the reviewers. Some information may be referenced to other sections of the application, or incorporated by reference, provided that these references are clear, specific, and essentially complete." SRP Section 8.4.3.1 states that an application would be acceptable if it addresses the baseline design criteria for chemical safety and includes information on the chemicals, process, equipment, inventories, ranges, and limits. At the construction permit stage, this would be expected to include design bases and values for these items, with sufficient system description to allow verification of the design bases and values. Sections 8.4.3.5 B, C, D, and F recommend that design bases, process safety features, and IROFS be included in the application.

Section 11.9.3.1 describes the nitric acid system. Apart from concentrations, no quantitative information is given. Inventories, temperatures, supply pressures, etc. are not provided. Tank and pump information that could affect safety are not described. Potential IROFSs are not identified although the text hints that some are present. This system also requires considerable interfacing between the local operator, local controls and the control room operator. Thus, human errors become a significant concern. The NRC would anticipate some form of reliability requirement in the design basis. Without this information, it is not possible to make a safety determination.

Response:

There are no safety functions provided by the nitric acid system with the exception of isolation and backflow prevention into the system. See the response to Question 196 for additional design detail.

Nitric Acid is received in the warehouse in a tote tank (DOT approved shipping container) containing a certified concentration of 63 Wt. % (13.6 N), which is well below 94.5 % concentration considered to be toxic and reactive per 29 CFR 1910.119 Appendix A.

Using procedures, the incoming concentration of nitric acid will be confirmed by independent testing prior to delivery to the reagents building for storage and use. Using volumetric totalizers, the 13.6 N nitric acid will be diluted with demineralized water to form 6 N and 1.5 N nitric acid solutions. Again, as part of the procedure, the prepared solution will be redundantly confirmed before use in the AP process.

These administrative controls will ensure that the Nitric Acid concentration does not exceed 94.5 Wt. % either in the reagents building or the BAP.

Action:

None

212. **<u>Section 11.9.3.1.2, 11.9-30</u>**

Assess the potential safety concerns and any safety requirements that might be associated with the pressurized 6N nitric acid tank.

Section 8.3 of the SRP states, "Information contained in the application should be of sufficient quality and detail to allow for an independent review, assessment, and verification by the reviewers. Some information may be referenced to other sections of the application, or incorporated by reference, provided that these references are clear, specific, and essentially complete."

Section 11.9.3.1.2 mentions that the 6N nitric acid tank is pressurized with air. No air pressure is specified. Figure 11.9-17 displays the system's flow diagram but does not show an air supply. It is unusual to pressurize a nitric acid tank and the impacts of the tank's rupture or unanticipated flow surges through lines and valves may impact the safe handling of radioactive materials. It is not possible to make a safety determination regarding this system until additional information is provided, including the design bases and values for the system and any controls.

Response:

The only principal SSC associated with this system is backflow prevention. See the response to Question 196 for a description of backflow prevention. Additional design information is provided below.

During normal operation of the AP process, the use of high pressure 6 N nitric acid is not required as the nitric acid is fed to the electrolyzer from atmospheric tanks by gravity. However, if one of the electrolyzers in the dissolution unit must be emptied for maintenance or repair (a very exceptional condition), the contents are temporarily manually transferred to the corresponding downstream 150 liter capacity geometrically safe slab tank, bypassing the filter that usually removes minute amounts of undissolved PuO_2. If the liquid were processed through the filter to remove the particulates, the undissolved PuO_2 particulates in the liquid could blind the filter and make the transfer impossible.

The electrolyzer has been designed and tested to prevent settling out of the particulates as they are dissolved; however, the slab tank is unable to maintain the particulates in suspension because of its required geometry and lack of mixing equipment. The result of this is that when the solution is returned back to the electrolyzer, many particulates may remain as residue in the bottom and on the sides of the slab tank. These must be resuspended in the smallest volume possible and transferred back to the other electrolyzer so that the particulate PuO_2 can be redissolved through normal process at the electrolyzer.

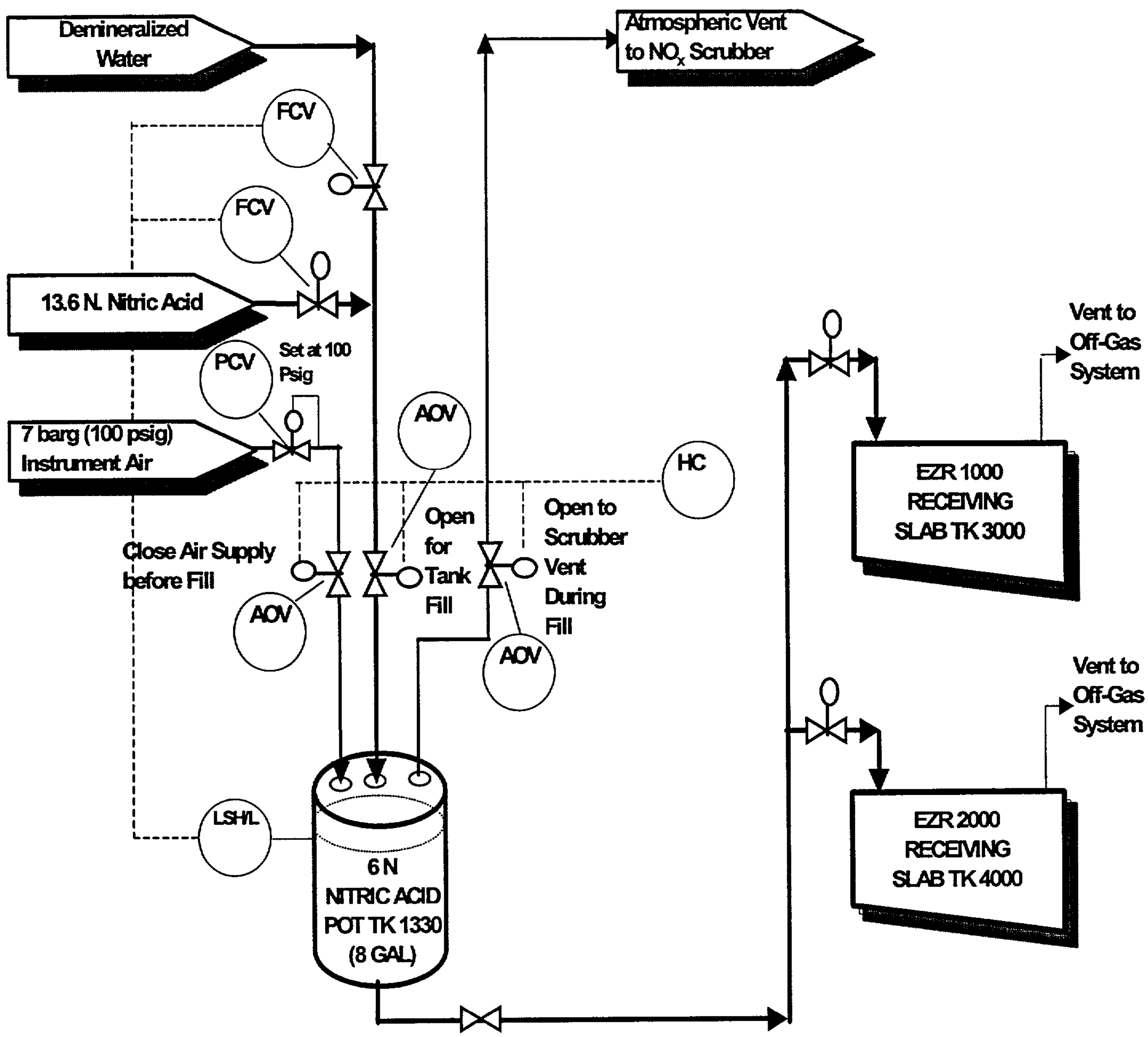
Resuspending the particulate PuO_2 requires the use of pressurized nitric acid to dislodge the particulates from the walls and bottom of the slab tank. Compressed air will be used to supply nitric acid from a dedicated nitric acid pot (see Sketch below). The pot and all connecting components will be designed for the 7 barg (100 psig) pressure condition, safely isolating the rest of the nitric acid system from the high pressure. All piping is already rated for 150 psig.

During the resuspensioning stage, the 100 psig nitric acid would be introduced into the tank in small amounts until, after two or three cycles of rinsing, all of the particulates are resuspended and returned to an electrolyzer. The volume is restricted due to the limited volume of the second electrolyzer.

The slab tank is unaffected by the pressure of the nitric acid as the pressure drops to system pressure (-2" W.C.) immediately on exiting from the inlet nozzle. The tank if vented directly to the offgas system that is maintained at an even more negative pressure. Thus, the only part of the system affected by the high pressure is the standby tank, the isolation valves, and piping.

Action:

The nitric acid system description in the CAR Section 11.9.3.1 will be revised.



6N NITRIC ACID PREPARATION AND DISTRIBUTION IN AQUEOUS POLISHING BUILDING

213. Section 11.9.3.10.1, p. 11.9-44

Describe the mixing of concentrated hydrazine hydrate and nitric acid.

Section 8.3 of the SRP states, "Information contained in the application should be of sufficient quality and detail to allow for an independent review, assessment, and verification by the reviewers. Some information may be referenced to other sections of the application, or incorporated by reference, provided that these references are clear, specific, and essentially complete." SRP Section 8.4.3.1 states that an application would be acceptable if it addresses the baseline design criteria for chemical safety and includes information on the chemicals, process, equipment, inventories, ranges, and limits. At the construction permit stage, this would be expected to include design bases and values for these items, with sufficient system description to allow verification of the design bases and values. Sections 8.4.3.5 B, C, D, and F recommend that design bases, process safety features, and IROFS be included in the application.

Section 11.9.3.10.1 mentions that the hydrazine system uses 35 percent hydrazine hydrate. The text indicates this is mixed directly with 13.6 M nitric acid in two reactors, each cooled with chilled water. These represent rather concentrated conditions for combining an oxidizing material with a fuel. Design basis information, such as enthalpy (heat) load, temperatures, potential IROFSs, etc. is needed before a safety determination can be made.

Response:

See the response to Question 125.

Action:

None

214. Section 11.9.4, pp. 11.9-49 thru 11.9-51

Clarify the design bases for non-principal SSCs and any impact these might have upon principal SSCs/IROFSs

Section 8.3 of the SRP states, "Information contained in the application should be of sufficient quality and detail to allow for an independent review, assessment, and verification by the reviewers. Some information may be referenced to other sections of the application, or incorporated by reference, provided that these references are clear, specific, and essentially complete." SRP Section 8.4.3.1 states that an application would be acceptable if it addresses the baseline design criteria for chemical safety and includes information on the chemicals, process, equipment, inventories, ranges, and limits. At the construction permit stage, this would be expected to include design bases and values for these items, with sufficient system description to allow verification of the design bases and values. Sections 8.4.3.5 B, C, D, and F recommend that design bases, process safety features, and IROFS be included in the application.

Section 11.9.4, "Design Basis for Non-Principal SSCs," is a listing of codes and standards. The section does not link specific codes and standards to specific SSCs and no design bases/values are provided. Some of the codes and standards overlap (e.g., on relief devices, pressure design). There is no discussion of the applicability of the codes in a nuclear facility. In addition, the distinction between non-safety SSCs and IROFSs is not clear. Some of the codes and standards would appear to also apply to potential IROFSs and non-safety SSCs might affect the function of IROFSs. For example, the plant uses compressed gas cylinders in several areas and as backup supplies for some functions (e.g., gas bottles for inerting, air scavenging). This section has several compressed gas standards that would seem to apply, but it is not clear how the linkage to an IROFS is addressed. More information is needed before a safety determination can be made.

Response:

Design bases of non-principal SSCs are provided for clarification of understanding. The design provides protection from non-principal SSCs to prevent interaction with principal SSCs. The principal SSCs for each utility system have been defined at the function level in the responses to the following Questions: 196, 200, 201,202, 203, 207, 208, 209, 210, and 211.

Action:

None

215. Section 11.9.5, pp. 11.9-51 and 11.9-52

Explain the separation of incompatible chemicals.

Section 8.3 of the SRP states, "Information contained in the application should be of sufficient quality and detail to allow for an independent review, assessment, and verification by the reviewers. Some information may be referenced to other sections of the application, or incorporated by reference, provided that these references are clear, specific, and essentially complete." SRP Section 8.4.3.1 states that an application would be acceptable if it addresses the baseline design criteria for chemical safety and includes information on the chemicals, process, equipment, inventories, ranges, and limits. At the construction permit stage, this would be expected to include design bases and values for these items, with sufficient system description to allow verification of the design bases and values. Sections 8.4.3.5 B, C, D, and F recommend that design bases, process safety features, and IROFS be included in the application.

Section 11.9.5 is entitled, "Design Basis for Principal SSCs," and consists of two short paragraphs. Portions of these paragraphs say:

> "Vessels/components are segregated/separated from incompatible chemicals ..."
>
> "Pressure vessels (e.g., gas storage bottles) are used in some utility systems. Principal SSCs are located away from these pressure vessels or otherwise protected such that failure of the pressure vessel will have no impact on the principal SSC."

Clear design bases, values, criteria, and descriptions (e.g., which components and pressure vessels) are needed before a safety determination can be made.

Response:

"Vessels/components are segregated/separated from incompatible chemicals ..."

Incompatible chemicals are broadly described as those chemicals that if blended together could react violently. Chemicals stored within the BAP are separated.

Incompatible chemical separation starts at receipt and storage of the chemical, during its preparation and, finally, transfer to process units using dedicated piping that are compatible with the specific chemical. By careful control from receipt through usage, incompatible chemicals are separated to prevent interaction.

Chemicals are supplied to MFFF at the lowest useable concentrations either as liquids or solids in bags. The chemicals are usually mixed with demineralized water and/or 6 N nitric acid to form a final concentration required by the process. Once prepared, the QA procedure requires that the prepared solution be redundantly tested independently before the control room can transfer the solution to the process vessel. These procedures are described in the response to Question 118.

For example, in Question 119, the use of 35 Wt. % hydrogen peroxide in 15-gallon containers is described. This is the lowest commercially available concentration and is well below the 52 Wt. % concentration that is considered to be toxic and reactive. Usage is small enough that only three 15-gallon capacity polyethylene containers are required to satisfy operation for more than one month. The hydrogen peroxide is supplied to the AP process users via continuous, all welded stainless steel lines that can be isolated on entry into the BAP using redundant seismic isolation valves (principal SSCs).

The considerations above apply to chemicals used in the AP process that originate in the BRP.

Some chemicals such as silver nitrate and manganese nitrate solutions are prepared directly in the BAP and are similarly tested prior to use by unit operations. Silver nitrate usage is reduced once the overall system is at equilibrium with the recovery of the silver being more than 98% effective. The manganese ion is a catalyst in the elimination of the oxalate ion in the oxalic mother liquors and its usage is consequently very small.

The NOX gas from dinitrogen tetroxide vaporization occurs at near ambient temperature to produce a low-pressure gas (1 bar) that is used directly in the oxidation column in the purification unit (also see Question 117 response). It can be isolated from the BAP using redundant seismically operated valves that are principal SSCs.

"Pressure vessels (e.g., gas storage bottles) are used in some utility systems. Principal SSCs are located away from these pressure vessels or otherwise protected such that failure of the pressure vessel will have no impact on the principal SSC."

See Question 204 for a detailed response.

Action:

None

216. Section 11.10, pp. 11.10-1 thru 11.10-2

Verify that there are no unidentified heavy lift applications, other than in the fresh fuel cask shipping area, including any cranes or hoists used for maintenance activities in the facility or on the MFFF grounds.

Section 11.4.8.2.F of the SRP states that the application should describe the bases for cranes based on an analysis that considers the confinement of radioactive material under conditions of system failure or misoperation. The reviewer must verify that only one heavy lift crane exists in the MOX facility.

Response:

There are no cranes that perform heavy lift applications presently identified as principal SSCs. There are however, non-principal SSC cranes that do perform heavy lift applications. As indicated in the CAR, the bridge crane in the fresh fuel cask shipping truck bay is the only identified heavy lift crane.

Action:

The next revision of the CAR will reflect the information above in an update to CAR Section 11.10.

217. <u>Section 11.10, pp. 11.10-1 thru 11.10-2</u>

Discuss how heavy lift crane(s) are prevented by design, interlocks, or administrative controls, from moving over safety, confinement, and other principle SSCs.

Section 11.4.8.2.C of the SRP states that the application should describe the methods used to prevent a heavy load from moving over a safety or containment system. The design principles preventing movement over safety, confinement, and other principle SSCs are not provided in the application.

Response:

Heavy lift cranes at the MFFF have not been identified as principal SSCs. The heavy lift crane identified in the CAR is not identified as moving over principal SSCs. In general, heavy lift cranes are prevented from moving over safety, confinement, and other principal SSCs by the following means:

- By design: the handling crane cannot physically access over a principal SSC, or is prevented by single failure proof interlocks from moving over principal SSCs.
- By administrative control: the handling crane must be in its withdrawn position if a load must be transferred below the crane, safe travel paths must be followed to prevent interactions with other principal SSCs, and lift height restrictions must be adhered to prevent lifts above design basis lift heights.

Specific controls will be identified in the ISA.

Action:

The CAR will be revised to reflect this information.

218. <u>Section 11.10, pp. 11.10-1 thru 11.10-2</u>

Assess the number of lifts of a fresh fuel cask container in any year and estimate the total percent of time during a lift a container could be above a principle SSC.

Section 11.4.8.2.E of the SRP recommends that information be provided to verify that the design and operation of heavy lift cranes fulfill all of the functional requirements of the integrated safety assessment. Information on handling fresh fuel cask containers is needed to assess the service conditions for the heavy lift crane in order to make a safety assessment of the unique application of this crane.

Response:

The frequency and duration of the lifts of fresh fuel casks are not an element of the safety bases. Load handling events involving fresh fuel casks are low consequence events because the cask does not break in the event of a drop.

Additional design information is as follows: Approximately 100 package lifts are expected in a year and approximately 33% of the duration of the lift may occur with the package over another package for a total of approximately 6 hours of lifts over another package. Fresh fuel casks are lifted over no principal SSCs other than another fresh fuel cask.

Action:

None

219. Section 11.10, pp. 11.10-1 thru 11.10-2

Discuss similar crane design and operating experience, including significant accidents, at La Hague and Melox facilities.

Section 11.4.8.2.F of the SRP recommends that information be provided to verify that heavy lift cranes have adequate reliability to perform their safety functions when needed. Information on crane failure rates, service conditions, and operating modes is needed to verify the design bases for heavy lift cranes.

Response:

La Hague operating T4 experience

T4 experience is provided here since R4, on which the AP process is mostly based, is not yet operational.

Notwithstanding that neither lifting failures nor load drops have occurred during T4 operation, operating experience from other La Hague facilities led to the following modifications to 5 Ton bridge cranes:

- For cranes having a handling frequency of greater than 1 per year, an active brake release control was added.
- For cranes having a handling frequency of less than 1 per year, an administrative control requiring the lifting mechanisms to be checked prior to use was added.

MELOX operating experience

Notwithstanding after 4 years of operation, no mechanical lifting failures have occurred, the following improvements have been implemented to two of the MELOX handling cranes:

- Shipping package gripper (receiving area) has been modified to improve load-positioning accuracy (non-safety-related modification).
- Shipping package handling crane (7.5 Ton, in shipping area) has been modified to allow for simultaneous horizontal and vertical motions to reduce the required time duration and operator exposure.

Action:

None

220. Section 11.10, pp. 11.10-1 thru 11.10-2

Clarify the location of the fresh fuel cask shipping area crane and discuss whether it should comply with ANSI/National Fire Protection Association (NFPA)-780-1986 standard for lightning protection for cranes.

Section 11.4.8.2.G of the SRP recommends that information be provided to show that the heavy lift cranes are based on codes and standards that represent a level of capability to meet design requirements. The standard for lightning protection is not discussed in the application.

Response:

The heavy lifting crane described by Section 11.10 (pp. 11.10-1 thru 11.10-2) is the 15 Ton (with 5 Ton Auxiliary hook) Truck Bay Bridge Crane that is located within, and is physically part of, the Fuel Truck Bay in D-101. Lightning should have no effect on the Truck Bay Bridge Crane because the lightning protection systems for the Shipping and Receiving Building will comply with the applicable requirements of NFPA 780-1997, as discussed in CAR Chapter 7. NFPA 780 does not apply to structures like a crane unless they are their own structure separate from other structures.

Action:

None

221. Section 11.10, pp. 11.10-1 thru 11.10-2

Evaluate the differences between the application-referenced design standards and those discussed in NUREG-0612, "Control of Heavy Loads at Nuclear Power Plants," for the following standards:

a) Crane Manufacturers Association of America (CMAA)-70, "Specifications for Top Running Bridge and Gantry Type Multiple Girder Electric Overhead Traveling Cranes," 1994 versus 1975 edition

b) American Society of Mechanical Engineers (ASME) B30.2, "Overhead and Gantry Cranes, " 1996 versus 1983 edition

c) ANSI N14.6, "Radioactive Materials - Special Lifting Devices for Shipping Containers Weighing 10,000 lbs or More," 1993 versus 1978 edition

d) ANSI/ASME B30.9, "Slings," 1996 versus 1971 edition.

NUREG-0612 references earlier standards. A change analysis for newer editions is needed. The reviewer must be able to find that these standards are an acceptable alternative to existing NRC guidance.

Response:

The heavy lift crane identified in CAR Section 11.10.2 is a non-principal SSC (CAR Section 11.10.7). In CAR Section 11.10.1, the reference to NUREG-0612 was intended to establish a common definition of a heavy lift crane and was not intended to commit to applying NUREG-0612. The discussion of codes and standards for the heavy-lift-crane in CAR Section 11.10.6 was provided to facilitate an understanding of the controls/requirements used to design the crane, and not as part of the design basis for principal SSCs.

Action:

None

222. Section 11.10, pp. 11.10-1 thru 11.10-2

Clarify the statements regarding the drop of a heavy load in Table 5A-6 and Table 5A-7 for events RD-6 and AS-8, respectively. In these cases, provide the weight of the postulated dropped loads. Explain the basis for the related load handling equipment being excluded from the list of heavy list cranes.

Section 11.4.8.2.E of the SRP recommends that information be provided to verify that the design and operation of heavy lift cranes fulfill all of the functional requirements of the integrated safety assessment. The application does not clearly state the loads or the bases for equipment being excluded from the designation, "heavy lift crane." The application should describe all heavy lift cranes and why some cranes that are related to defense-in-depth are excluded.

Response:

DCS assumes the question is related to event RD-9 instead of RD-6 on Table 5A-7.

This question appears to have been asked due to an inappropriate use of the term "heavy load" in the tables cited. There are no heavy loads handled above either the cladding or assembly process equipment that would require the associated load handling equipment to be subject to NUREG-0612 provisions.

Action:

The table will be revised to delete the word "heavy" in the next CAR revision.

223. Section 11.11, pp. 11.11-1 thru 11.11-23

Clarify the design basis for safety in the Laboratory.

Section 8.3 of the SRP states, "Information contained in the application should be of sufficient quality and detail to allow for an independent review, assessment, and verification by the reviewers. Some information may be referenced to other sections of the application, or incorporated by reference, provided that these references are clear, specific, and essentially complete." SRP Section 8.4.3.1 states that an application would be acceptable if it addresses the baseline design criteria for chemical safety and includes information on the chemicals, process, equipment, inventories, ranges, and limits. At the construction permit stage, this would be expected to include design bases and values for these items, with sufficient system description to allow verification of the design bases and values. Sections 8.4.3.5 B, C, D, and F recommend that design bases, process safety features, and IROFS be included in the application.

Section 11.11 discusses the laboratory. The laboratory plans on manual operations and pneumatic delivery of solid and liquid samples. The laboratory consists of several gloveboxes linked together, and includes analytical stations, instruments, and a MOX pellet test line. The test line reproduces the main steps of the fabrication process for adjustment of process parameters and characterization of pellet blends. Design basis information is not provided for the laboratory. For example, the NRC would anticipate communication of estimates of the number of samples, the operator actions with those samples, human and instrument errors, and required reliabilities. Inventory information would also be anticipated; Table 5.5-2 shows an entry for a laboratory inventory of 200 grams as plutonium dioxide powder. The laboratory would also have pellets and liquid samples containing plutonium. Each pellet weighs about 5 grams and contains about 0.25 grams of plutonium. In the absence of additional information, it is not possible to confirm the inventory estimate. The laboratory also has a liquid waste processing unit consisting of four small tanks (15.8 gallons each); the design basis and any concentration limits are not provided. This information is needed before a safety determination can be made.

Response:

As noted above, a description of the MFFF laboratory is provided in CAR Section 11.11. The descriptions of chemical process safety included in CAR Chapter 8, as well as glovebox descriptions and design bases of CAR Section 11.4.7.1, also apply to the MFFF laboratory. The following principal SSCs discussed in CAR Chapter 5 and listed in CAR Table 5.6-1 are applicable to the MFFF laboratory:

- C4 Confinement System
- Chemical Safety Controls
- Combustible Loading Controls
- Criticality Controls
- Fire Barriers

- Fire Detection and Suppression
- Fluid Transfer Systems
- Glovebox
- Glovebox Pressure Controls
- Material Handling Controls
- Material Handling Equipment
- Material Maintenance and Surveillance Programs
- Process Safety I&C System
- Training and Procedures.

Detailed MOX process hazard evaluations (What If/HAZOP) performed in support of the Integrated Safety Assessment will identify specific IROFS associated with the MFFF laboratory. MFFF laboratory chemical inventories are provided in the response to Question 113. Tables 1 and 2 below provide a description of MFFF laboratory sample analyses. Information includes MFFF AP and MP samples, sampling frequencies, sample quantities, and laboratory analysis types. Tables 3 and 4 below provide information concerning laboratory incoming and outgoing products respectively. A brief description of the laboratory liquid and solid waste processing follows:

The MFFF laboratory provides liquid waste processing capabilities for analytical effluents. These liquid effluents are manually transferred from the analytical lines to the liquid waste processing line. They are packaged in 1-liter bottles and emptied into the suitable tank according to their origin (Purification (KPA) or Acid Recovery (KPC) recycling). The liquid waste processing station is composed of four 60 liter buffer tanks that collect the laboratory effluent generated by analyses:

- 2 tanks to collect solutions that are transferred to Purification (KPA):
  - 1 to collect and treat solutions
  - 1 to transfer the solutions to AP area after analysis
- 1 tank to collect solutions that are transferred to Acid Recovery (KPC)
- 1 tank to collect solutions that could be transferred to Liquid Waste Reception (KWD)

Each tank is equipped with:

- A funnel for manual introduction of analytical effluents
- A pump to transfer or homogenize the solutions
- A sampling point for solutions characteristics analysis prior to transfer
- Level sensors

Laboratory solid waste processing consists of:

- Recovering scrap material from coated pellets and crucibles for recycling into production units
- Effluent treatment to obtain a solid matrix that can be stored as waste. This operation is only performed on very low Pu content solutions whose characteristics are not in compliance with production criteria

Action:

Clarify the above information in the next update of the CAR.

Table 1. MFFF Laboratory Sample Analysis Description

Product Type	Analyses Required	Analytical Principle	Average Sampling Frequency

Table 1. MFFF Laboratory Sample Analysis Description

Product Type	Analyses Required	Analytical Principle	Average Sampling Frequency

Table 1. MFFF Laboratory Sample Analysis Description

Product Type	Analyses Required	Analytical Principle	Average Sampling Frequency

	Pu isotopic composition	Mass spectrometry	
	H_2O content determination	Gravimetry	
	Grain size determination	Coulter counter	
	Specific surface area	Adsorption of liquid N_2	
	Impurities Concentration	Inductive coupled plasma - Mass spectrometry, Alpha spectrometry, Spectrophotometry, Titration after pyrohydrolysis	
	Characterization of gamma emitters	Gamma spectrometry	

Table 2. MFFF Laboratory AP Sample Analysis Description

Unit	Equipment		Sampling number	Sampling type	Solution nature	Activity mCi/l	Composition	Determinations	Frequency		Observations
	No.	Function							Periodicity	Exceptional	

Table 2. MFFF Laboratory AP Sample Analysis Description

Unit	Equipment		Sampling number	Sampling type	Solution nature	Activity mCi/l	Composition	Determinations	Frequency		Observations
	No.	Function							Periodicity	Exceptional	

Table 2. MFFF Laboratory AP Sample Analysis Description

Unit	Equipment		Sampling number	Sampling type	Solution nature	Activity mCi/l	Composition	Determinations	Frequency		Observations
	No.	Function							Periodicity	Exceptional	

Table 2. MFFF Laboratory AP Sample Analysis Description

Unit	Equipment		Sampling number	Sampling type	Solution nature	Activity mCi/l	Composition	Determinations	Frequency		Observations
	No.	Function							Periodicity	Exceptional	

Table 2. MFFF Laboratory AP Sample Analysis Description

Unit	Equipment		Sampling number	Sampling type	Solution nature	Activity mCi/l	Composition	Determinations	Frequency		Observations
	No.	Function							Periodicity	Exceptional	

Table 2. MFFF Laboratory AP Sample Analysis Description

Unit	Equipment		Sampling number	Sampling type	Solution nature	Activity mCi/l	Composition	Determinations	Frequency		Observations
	No.	Function							Periodicity	Exceptional	

Table 2. MFFF Laboratory AP Sample Analysis Description

Unit	Equipment		Sampling number	Sampling type	Solution nature	Activity mCi/l	Composition	Determinations	Frequency		Observations
	No.	Function							Periodicity	Exceptional	

Table 2. MFFF Laboratory AP Sample Analysis Description

Unit	Equipment		Sampling number	Sampling type	Solution nature	Activity mCi/l	Composition	Determinations	Frequency		Observations
	No.	Function							Periodicity	Exceptional	

Table 3. MFFF Laboratory Incoming Products

Received From	Material	Sample Quantity

Table 4. MFFF Laboratory Outgoing Products

Originated	Material	Destination

CHAPTER 12, HUMAN FACTORS ENGINEERING FOR PERSONNEL ACTIVITIES

224. Section 12.1, pp. 12-1 thru 12-2

Discuss the human factors/human performance activities associated with maintenance of automated systems used in the MFFF, and identify any safety significant human-system maintenance interfaces.

Section 12.1 of the SRP defines "personnel activities" as activities identified as items relied on for safety (IROFS) and personnel activities that support safety such as maintenance.

Response:

The ISA process will identify the sensors, instruments, and actuators that are classified as IROFS. The appropriate human-system interface requirements will be identified, and the human performance requirements will be established during the detailed design process. Activities associated with the maintenance or operation of the instruments, sensors and actuators classified as IROFS will be evaluated for Human Factors attributes using the criteria of IEEE Std 1023, *IEEE Guidelines for the Application of Human Factors Engineering to Systems and Equipment, and Facilities of Nuclear Power Generating Facilities.*

While IEEE Std 1023 is specifically applicable to the design of the human-system interface for safety systems found in nuclear power plants, the Human Factors Engineering characteristics identified in Section 4 of the standard are generally applicable to the design of IROFS that are found in the MFFF, recognizing that there are conditions, systems, operating requirements and consequences unique to a nuclear plant and not found in a fuel fabrication facility.

The NUREG/CR-6636 Design Review Checklist will be used in the design and review process.

Action:

None

225. Section 12.1, pp. 12-1 thru 12-2

Describe the criteria and basis used for determining that the protective control subsystem does not constitute a significant human-system interface. Define what "significant" means.

Regulatory Acceptance Criterion A of Chapter 12 of the SRP recommends that the applicant appropriately identify personnel activities so that the reviewer can understand the actions, the human-system interfaces involved and the consequences. It is, therefore, important to understand why the protective control subsystem does not constitute a significant human-system interface.

Response:

The protective control subsystem is designed to satisfy industrial safety requirements and is not a principal SSC.

The protective control subsystem's Human-System Interface (HSI) is limited to the sensors required to implement the protective actions required by 29 CFR 1910; the supervisory interfaces required to reset a system that has been locked out by a trip of a protective system sensor; and the programming interface required to load software into the controllers (i.e., in the event that programmable electronic systems are used as protective controllers).

Action:

None

226. Section 12.1, pp. 12-1 thru 12-2

While the MFFF has a high level of automation with operators mainly monitoring the operation of systems and exercising supervisory control only when necessary, describe how staff are alerted to undesirable conditions at control stations that are not normally staffed, and what criteria are used to decide when appropriate operations staff need to be at these remote locations for appropriate and timely response.

Regulatory Acceptance Criterion F of Chapter 12 of the SRP requires the applicant to review the number and qualifications of personnel for each personnel activity during all plant operating conditions in a systematic manner. The criteria used to decide what staff need to be at these remote locations and when ensures appropriate staffing based on this systematic review.

Response:

In the automated areas of the MFFF, the performance of the systems are constantly monitored by the automation supervisory systems. One of the attributes of the functional units monitored by the supervisory system is the state of an automated activity. If an activity is not concluded in an anticipated state or within an expected time, or if a continuous process is not within allowed limits, an alarm is generated in the control room for that functional unit.

The design of the MFFF establishes several different control rooms and control of the various functional units of the MFFF are grouped together into these control rooms. If a functional unit is in operation, the control room associated with that functional unit is occupied. If none of the functional units assigned to a particular control room are operating, that control room may not be occupied. For example, control outputs for the fissile material mass accounting system are not needed if there are no movements into, out of, or within a glovebox; similarly, the mass measurement system and the mass limit alarms are not meaningful. Signals for functions appropriate only to an operational functional unit will be transmitted to the control room that is assigned to that function. Signals appropriate to a facility function, such as the HVAC system, will be transmitted to the D301 control room, which is continuously occupied.

Control room D301 contains supervisory monitoring capability for MFFF features and systems that require full time monitoring. Monitoring of conditions that must be made continuously available at all times to the operations staff will be provided in the D301 control room or, in the case of Items Relied On For Safety, will also be made available in the emergency control rooms, D318 (train A) and D319 (train B).

The performance of facility system items that are relied on for safety are continuously monitored. The performance monitoring sensors and instruments are connected to the emergency control rooms. Any alarm generated by an Items Relied On For Safety is sent to the emergency control rooms. These alarm signals are repeated in the D301 control room.

Staffing evaluations will be completed during the detailed design phase and will be derived from the staffing requirements that exist in the La Hague and MELOX facilities. This will be provided with the license application for possession and use of special nuclear material.

Action:

None

227. Section 12.1, pp. 12-1 thru 12-2

The applicant states that "in general, omission of an operator action does not result in adverse conditions, and that errors in operator actions are generally expected to be bounded by other deterministic design basis accident assumptions." Clarify what is meant by "in general," and describe by example what the other deterministic design basis assumptions are.

This statement is confusing and provides little information about the deterministic design basis assumptions actually used.

Response:

There are no safety events that require immediate operator action to mitigate the consequences to below the performance criteria of 10 CFR 70.61. Operators primarily perform monitoring activities in response to emergency conditions. The AP and MP processes are designed to shut down during upset conditions.

For normal operations, the operators perform a supervisory role with respect to the automated systems.

No scenario has been identified where omission of an operator action results in adverse conditions, and errors in operator actions have been anticipated in the system design while considering other deterministic design basis accident assumptions and scenarios.

An Integrated Safety Analysis (ISA) will be performed to assess the safety basis of the principal SSCs at the MFFF. The ISA includes an analysis of internal, man-made-external, and natural phenomena hazards. A subset of the events analyzed within the ISA involves personnel actions that have the potential to create event sequences that may affect nuclear safety. The ISA will include a single failure evaluation that includes the operator actions.

Action:

The CAR will be revised to reflect the above discussion.

228. Section 12.2.1, p. 12-2

Verify the commitment to use NUREG-0711 to guide their human factors design basis development work during construction and evaluate the revision to IEEE 1023.

IEEE 1023 (1988), "IEEE Guidelines for the Application of Human Factors Engineering to Systems and Equipment and Facilities of Nuclear Power Generating Facilities," will be used during construction, design and startup of the MFFF. This standard is being revised and should be issued in 2002. Also, Section 12.7 References, of Chapter 12 of the SRP, includes NUREG-0711, "Human Factors Engineering Program Review Model." The applicant indicated in an April 25, 2001, meeting with NRC staff, that it would also use NUREG-0711 to guide their human factors design basis development work during construction and evaluate the revision to IEEE 1023.

Response:

DCS indicated to the staff in the April 25, 2001, meeting with the NRC that NUREG-0711 would be reviewed for insight into the review process. However, DCS has not committed to NUREG-0711 because it describes a design and review process that is applicable to the single step licensing of advanced reactors and is not applicable to a 10 CFR 70 facility. IEEE Std 1023-1988 will be used as the basis standard for the MFFF.

Any revised issue of IEEE Std 1023 will have to be evaluated by DCS before DCS can make any comment on the applicability of the revised standard to the design of the MFFF.

Action:

None

229. Section 12.2.1, p. 12-2

Identify and describe what "facility baseline design" means, or cross-reference to other appropriate Chapter(s) of the application.

Response:

"Facility baseline design" is synonymous with the technical baseline defined in the configuration management policies, Section 15.2.1 of the CAR.

Action:

None

230. Section 12.2.1, p. 12-2

Identify and describe the aspects of the design that reduce the risk of errors or challenges to principal SSCs, and how these aspects are evaluated.

Section 12.3 "Areas of Review" of the SRP recommends that the applicant describe safety-significant personnel actions, the associated human systems interfaces, and the consequences of incorrectly performing or omitting actions for each personnel activity.

Response:

The MFFF is designed to maximize the use of automation, thus minimizing human operations and interactions with the MFFF SSCs. By reducing these interactions, the probability of a human caused error being introduced is reduced.

As the designs for the MFFF functional units are developed, the functional units will be analyzed in the ISA process to identify safety significant conditions and actions that might be required.

An Integrated Safety Analysis (ISA) will be performed to assess the safety basis of the principal SSCs at the MFFF. The ISA includes an analysis of internal, man-made-external, and natural phenomena hazards. A subset of the events analyzed within the ISA involves personnel actions that have the potential to create event sequences that may affect nuclear safety. The ISA will include a single failure evaluation that includes the operator actions.

Action:

None

231. Sections 12.2.3, 12.2.3.1, and 12.2.3.2, pp. 12-3 thru 12-4

Describe, by example, how operating experience of the La Hague and MELOX facilities is incorporated in the MFFF design process. Provide lessons-learned evaluations that show how the MFFF as a next generation facility effectively incorporates this operating experience.

Regulatory Acceptance Criterion C of the SRP requires the applicant to identify safety-related human factors engineering events or potential events that have occurred in existing facilities that are similar to the MFFF.

Response:

The final HFE review of the MFFF will be an integrated system validation of personnel activities relied on for safety including, but not limited to, human-system interfaces, procedure development, training development, staffing, and maintenance tasks. The human performance activities identified in the functional allocations and task analysis will be updated to reflect the final results of the ISA.

The MFFF is not considered a "next generation" facility, but is designed using existing and proven technology as much as possible. Doing so provides the benefit of the operational experience that is available from the operating facilities. Participation in MFFF development by personnel familiar with MELOX and La Hague design and operation is the primary means of incorporating operating experience from these facilities into the MFFF design.

During the operational phase of the MFFF, the operational experiences of the MFFF will become part of the continuing review of the facility as specified in Section 6.3 of IEEE Std 1023.

Action:

None

232. Sections 12.2.3, 12.2.3.1, and 12.2.3.2, pp. 12-3 thru 12-4

The applicant indicated it will use the review criteria of NUREG-0700, Rev. 1, to evaluate the MFFF human-system interfaces. NRC staff plans to issue NUREG-0700, Rev. 2, in March 2002. This revision will include human factors engineering guidance to account for emerging technologies and increased automation, including digital systems and systems comprised of both analog and digital technology, e.g., hybrid control rooms. Also, the "Reference" section of Chapter 12 of the SRP includes five NUREG/CR reports (NUREG/CRs-6633-6637) that contain technical bases and guidance for risk-significant hybrid control room human performance issues. The applicant indicated in the April 25, 2001, meeting with the NRC staff, that it would use both NUREG-0700, Rev. 2, and the referenced NUREG/CR reports in both preliminary and final design. The applicant should verify this commitment.

Response:

At the April 25, 2001, meeting between DCS and the NRC, DCS indicated to the Staff that later revisions of NUREG-0700 would be reviewed for applicability to the MFFF. DCS will use the cited NUREG/CR reports as guidance.

Action:

Future revisions of NUREG-0700 will be evaluated for applicability when available.

233. Section 12.3, pp. 12-3 thru 12-5

Clarify what is meant by "no additional formal operating experience review is anticipated," for the MFFF based on the operational experience at the La Hague and MELOX facilities previously incorporated in the MFFF design. Lessons-learned from operating experience should be a continuing activity throughout construction, detailed design, and operation.

Regulatory Acceptance Criterion C of the SRP recommends that the applicant identify safety-related human factors engineering events or potential events that have occurred in existing facilities that are similar to the MFFF.

Response:

The MFFF design is based on the design of COGEMA's existing MELOX and La Hague facilities. These facilities represent a significant body of human factors experience. A fundamental design requirement of the MFFF project is to maximize the use of existing proven technologies in process and facility design.

Operational experiences of similar facilities will be reviewed for applicability to the MFFF.

During the operational phase of the MFFF, the operational experiences of the MFFF will become part of the continuing review of the facility as specified in Section 6.3 of IEEE Std 1023.

Action:

None

CHAPTER 15, MANAGEMENT MEASURES

234. Section 15.1, pp. 15-1 thru 15-5

Amplify the application and definitions of Quality Levels (QL) presented in the Section 15.1 of the application. Also, provide a full description of the methods for grading the application of quality assurance (QA) controls for various QLs.

SRP 15.1.4.3, Regulatory Acceptance Criteria, states that the applicant should describe, if used, the graded approach for application of QA. The methods for grading should be described, including how the QA program controls are applied or not. Amplify the discussion of the definitions of QL-1, QL-2 and QL-3. Discuss the relationship between the QL definitions and designations and the performance criteria of 10 CFR 70.61, and to what extent probability performance or failure rates are factored in the application of QLs and QA controls. Please explain the relationships and differences between the QL and applied QA controls and the engineering requirements and specifications for QL-1 and -2 SSCs.

Examples may be used for illustrative purposes. For example, specifically identify which Mixed Oxide Project Quality Assurance Plan (MPQAP) provisions will apply to criticality controls classified QL-1b. It would appear that most criticality safety controls would be graded QL-1b, on account of the double contingency principle. It is stated in the QAP that all MPQAP requirements pertain to controls graded QL-1a but, but not necessarily QL-1b. This information is necessary to ensure that the quality assurance program provides reasonable assurance of protection against a criticality accident. Identify the differences in the application of QA controls for SSCs that are produced routinely or to standard requirements such as thermocouples and those which may be customized such as electrolyzer controls.

Response:

Question 4 of the NRC's "Request for Additional Information on the Duke Cogema Stone & Webster (DCS) Mixed Oxide Project Quality Assurance Plan, Revision 2" (NRC letter dated 6/19/01) requested the same information. See the DCS response to that question in DCS letter dated 7/18/01, DCS-NRC-000054, "Response to NRC Request for Additional Information on MOX Project Quality Assurance Plan (MPQAP) Revision 2".

In addition, the following information is to further clarify the process and criteria for grading IROFS and QL-2 SSCs under the QA program.

General Discussion

Grading refers to the selection of QA controls. Graded QA provides a safety benefit by allowing DCS and the NRC to preferentially allocate resources based on the safety significance of SSCs. Grading an SSC will not degrade its performance or prevent it from meeting its intended safety function. The QA grading process is implemented to match the necessary QA controls with SSC safety significance so that technical, engineering, design and safety requirements are met.

The requirements delineated in Appendix B to 10 CFR Part 50 recognize that QA program controls should be applied in a manner consistent with the importance to safety of the associated structures, systems, and components (SSCs). Because the quality level of an SSC is determined by the role of the SSC in meeting the performance requirements of 10 CFR 70.61 (which provides the Part 70 definition of items relied on for safety [IROFS]), the quality level also serves as an indicator of the safety significance of the SSC in the context of grading. Additional SSCs that are not IROFS, but which help minimize risk below the criteria of 10 CFR 70.61, are also controlled under selected elements of the DCS QA program (i.e., under QL-2). These SSCs are not required to demonstrate safety in the context of Part 70, but are controlled voluntarily as "augmented quality provisions."

QL-1a SSCs are not typically graded; QL-1b and -2 SSCs are graded as discussed below.

Initial Assignment of SSC Quality Levels

MFFF SSCs are assigned a quality level (QL) commensurate with each SSC's function and safety significance. The initial QL designations (or QA classifications) of SSCs were established at a functional level based on engineering review of the following:

- design criteria and design requirements;
- safety significance relative to 10CFR70.61 performance requirements;
- consideration of failure consequences (i.e., single failure vs. defense in depth);
- consideration of the MELOX and La Hague design and operating experience; and
- MPQAP Section 2.2.1 definitions for quality levels.

This review resulted in a deterministic QL designation for each SSC. This QL was documented and controlled in a "functional classification list" as part of the design hierarchy, and on the applicable design documents, to indicate where QA controls were needed during initial design development. Upon completion of the safety assessment of the design bases of principal SSCs and the Integrated Safety Analysis (ISA), these initial SSC quality level assignments will be either confirmed or changed. Changes to quality level designations necessitates re-evaluation of any QA grading applied up to that time (see "Feedback Mechanisms and Reassessing Safety Significance" below).

Grading Process

DCS consulted the applicable provisions of Regulatory Guide 1.176, *An Approach for Plant-Specific, Risk-Informed Decisionmaking: Graded Quality Assurance*, and NRC Inspection Procedure 35703, *Graded Quality Assurance*, to develop the process and criteria for grading SSCs. These documents are focused on *changes* to existing *reactor* quality programs on the basis of formal *probabilistic risk assessments* performed for those facilities, and are therefore not directly applicable to the MFFF process. However, they provide some guidance in the development of a framework for the grading process and for the establishment of criteria for determining which 10 CFR 50 Appendix B controls apply to SSCs with limited safety significance.

The classification process consists of assigning a quality level (QL) to an SSC on the basis of its role in meeting 10 CFR 70.61 performance requirements (i.e., QL-1 for IROFS). Certain non-IROFS are also included in the QA program (i.e., as QL-2) if they serve to minimize certain risks below the 10 CFR 70.61 performance requirements. (QL-3 is used to identify SSCs with non-regulatory programmatic importance, such as investment protection or production capacity, and are not discussed here, as they have no bearing on the safety or licensing bases for the MFFF. Similarly, QL-4 SSCs are not discussed here, as QL-4 is simply a designation indicating the QA program is not applicable.)

Quality levels are defined in the MPQAP.

While a direct correlation between QLs and safety-significance thresholds in Regulatory Guide 1.176 does not exist, it is informative to compare them as follows:

- QL-1a is used to designate MFFF SSCs whose single failure could cause an accident with consequence exceeding the 10 CFR 70.61 performance criteria. This designation is comparable to "high safety significance" described in Regulatory Guide 1.176.

- QL-1b is used to designate MFFF SSCs whose failure could indirectly lead to exceeding 10 CFR 70.61 performance criteria (i.e., failure in conjunction with an independent, unlikely failure of another item or administrative control). This designation is comparable to "medium safety significance" described in Regulatory Guide 1.176.[1]

- QL-2 is used to designate SSCs that do not contribute to safety as defined in 10 CFR 70, but which minimize risk below the performance thresholds of 10 CFR 70.61. This designation is comparable to "low safety significance" in that the SSCs, by definition, are not relied on for safety.

The grading process defines the selection of QA controls on the basis of SSCs' safety significance. The MPQAP controls are evaluated for SSCs or categories of SSCs based on their quality levels and functional requirements. The grading process reflects the criteria used for determining which MPQAP requirements are not applicable to IROFS and QL-2 SSCs as described below.

The grading process is conducted by design, safety, and quality assurance personnel, and is documented in an engineering analysis subject to review and approval by both engineering and QA management in accordance with QA procedures. Grading analyses will apply to QL-1b and -2 SSCs.

---

[1] Regulatory Guide 1.176 includes discussion that indicates that the diversity of systems that are able to fulfill critical high level functions (e.g., reactivity control, decay heat removal) can have the result that each individual system could meet all quantitative guidelines to be categorized in the low safety-significance group. The guidance indicates that the licensee is expected to designate at least one system associated with critical high-level functions as high safety significant. DCS complies with this guidance by (a) providing that "critical high-level" safety functions of confinement and single-failure-prone criticality (if any) are QL-1a; (b) designating all "sole IROFS" as QL-1a; and (c) *not* taking credit for single-failure-based redundancy in determining QL-1b designations (i.e., if an SSC is one of two active components providing the same function, it is still designated as QL-1a).

Grading Criteria

The evaluation of SSCs for selection of QA controls takes into account the following considerations:

- the function or end use of the SSC;
- the consequence of failure of the SSC;
- the importance of the data being collected or analyzed by the SSC;
- the complexity of design or fabrication of the item or design or implementation of the activity;
- the reliability of the associated processes;
- the reproducibility of results;
- the uniqueness of the item or service quality;
- the necessity for special controls or processes; and
- the degree to which functional compliance can be demonstrated through inspection or test;

along with any other relevant factors, including program risk, as applicable. As examples of the above considerations:

- An SSC whose safety function is not specifically credited in safety analyses (i.e., an SSC designated as IROFS solely on the basis of defense in depth) is considered QL-1b and subject to graded controls. This conclusion reflects consideration of the function/end use of the SSC and the consequences of its failure as indicated in MFFF safety analyses.

- An IROFS that is specifically engineered for the MFFF, such as a glovebox, will not likely be graded (i.e., QL-1a), but rather subject to all applicable 10 CFR 50 Appendix B criteria, in contrast to a thermocouple that is IROFS but is readily available "off the shelf" (assuming its safety significance does not otherwise preclude grading). This conclusion reflects consideration of the comparative complexity and uniqueness of the SSCs.

Regulatory Guide 1.176 identifies the following 10 CFR 50 Appendix B criteria as candidates for grading:

- Procurement;
- Inspection;
- Records and Documentation;
- Audits;
- Staff Training and Qualification;
- Corrective Action; and

- Design.

These criteria, and the basis for grading them as indicated in Regulatory Guide 1.176, will be appropriately considered in the detailed grading analyses currently in progress.

QL-1 SSCs (QL-1a and QL-1b)

QL-1a SSCs and their associated activities (to prevent or mitigate a postulated confinement or criticality accident) are subject to all the requirements in sections 1-18 of the MPQAP. No grading of QA controls applies to QL-1a SSCs (unless justified on a case-by-case basis in discrete SSC-specific analyses; this is expected to be very rare, and no instances have been identified to date).

QL-1b SSCs and their associated activities (criticality controls subject to double contingency, except for geometry control, and SSCs that provide defense-in-depth) are evaluated against the requirements in sections 1-18 of the MPQAP. Based on the SSC's function, this evaluation determines which (if any) MPQAP requirements are not applicable or are only partially applicable (i.e., are not required to provide assurance the SSC will perform its intended function). Since the single failure of a QL-1b SSC cannot, by definition, result in exceeding 10 CFR 70.61 performance requirements, they have more potential to be graded. Justification for grading these SSCs may include unnecessary credit attributed to the SSC in the ISA; application of additional control from other SSCs or management measures; and industry precedent in justifying exclusion or partial application.

QL-2 SSCs

QL-2 SSCs and their associated activities – i.e., those SSCs that provide support of normal operations of the facility (e.g., occupational exposure, radioactive waste management) and SSCs that minimize public, worker, and environmental risks below 10 CFR 70.61 performance criteria (e.g., physical interaction protection, radiological and criticality alarms) – are also evaluated against the requirements in sections 1-18 of the MPQAP. This evaluation identifies which QA controls are needed to ensure these SSCs meet their intended functions. (This evaluation may also include nuclear industry precedent in the application of augmented QA requirements.)

Application of Graded QA Controls

QA grading analyses for QL-1a, QL-1b and QL-2 SSCs are used to identify QA requirements to the design, construction, and (later) operation of these SSCs. These requirements are reflected in applicable project procedures, analyses, specifications, and other QA program documents. Revision and approval of these documents is in accordance with applicable procedures.

Feedback Mechanisms and Reassessing Safety Significance

Changes in quality level classification of an SSC will necessitate re-evaluation of assigned QA controls. Changes to quality levels may result from ISA completion, design changes (including changes to safety significance), or elevation to a higher quality level by management decision.

Quality level classification changes require updating of the applicable design documents for the particular SSC that was changed. These changes necessitate review of applicable QA requirements for confirming or changing the previously established graded QA controls. Affected documents are revised in accordance with the requirements of the controlling procedures for the specific documents.

See the response to the MPQAP RAI question 4 submitted by DCS to the NRC 18 July 2001 (Letter Number DCS-NRC-000054) for additional discussion of the relationship between the QL definitions and the performance criteria of 10 CFR 70.61, and examples used for illustrative purposes.

Action

Revise the MPQAP to reflect the discussion above and clarify the application of the graded QA program to QL-1 and -2 SSCs.

235. <u>Section 15.1, pp. 15-1 thru 15-5</u>

Clarify what is meant in MPQAP Table 2-1 by "a condition compromising criticality safety", and explain the differences or discrepancies between this statement and the CAR Section 15.1.6.2 statement regarding SSCs whose single failure can directly result either in a criticality.

SRP Section 15.1.4.3, "Regulatory Acceptance Criteria," states that the applicant should describe, if used, the graded approach for application of QA. Section 15.1.6.2 states that "SSCs whose single failure can directly result in...a criticality accident...are designated QL-1a." However, MPQAP Table 2-1 states that QL-1a controls are those which can cause "a condition compromising criticality safety." This information is necessary to ensure that the quality assurance program provides reasonable assurance of protection against a criticality accident.

Response:

Question 5 of the NRC's "Request for Additional Information on the Duke Cogema Stone & Webster (DCS) Mixed Oxide Project Quality Assurance Plan, Revision 2" (NRC letter dated 6/19/01) requested the same information. See the DCS response to that question in DCS letter dated 7/18/01, DCS-NRC-000054, "Response to NRC Request for Additional Information on MOX Project Quality Assurance Plan (MPQAP) Revision 2".

Action:

None

236. <u>Section 15.1, pp. 15-1 thru 15-5</u>

Discuss the meaning and use of the QL-3/QL-1 boundary flags on drawings. Identify which components are QL-1 and which are QL-3 on drawings such as that in Figure 11.4-11 of the application.

SRP Section 15.1.4.3, "Regulatory Acceptance Criteria," states that the applicant should describe, if used, the graded approach for application of QA. Note 2 to Figure 11.4-11 in the applications states that, "This drawing contains QL-1 IROFS & QL-3 components."

Response:

The QL-3/QL-1 boundary flags shown on CAR Figure 11.4-11 establish the boundaries where the Quality Level requirements change from QL-1 to QL-3 based on the safety functions established for the MFFF ventilation systems. For example, the Supply Air System (HSA) does not perform a safety function, except for supporting the heat removal function for rooms which remain in operation during a loss of off-site power or emergency operating conditions. Figure 11.4-11 shows the redundant Quality Level 1 dampers which isolate the Quality Level 3 portions of the Supply Air System, and the Quality Level 1 dampers which open the emergency bypass, allowing the Quality Level 1 High Depressurization Exhaust (HDE) to draw outside air through rooms requiring heat removal. The boundary flags are used on the design drawings to establish the quality levels for components shown on the drawing. During the final design phase of the project, a Master Equipment List will be prepared based on the drawing information. This Master Equipment List will list individual components and will identify their Quality Levels.

The graded approach for the application of QA is described in the response to Question 234 and in the MOX Project Quality Assurance Plan.

Action:

None

237. Section 15.1, pp. 15-1 thru 15-5

Provide justification for classification of the criticality monitoring and criticality alarms as QL-2 and not QL-1.

SRP Section 15.1.4.3, "Regulatory Acceptance Criteria," states that the applicant should describe, if used, the graded approach for application of QA. In processes dealing with liquids, it is possible to get a pulsating cycle between critical and non-critical conditions, and as such, criticality monitors and alarms could be considered to be mitigating IROFS. Please discuss the functions and/or importance of criticality monitors and alarms for prevention of or mitigation for a pulsating criticality.

Response:

The requirement for a criticality monitoring and alarm system (10 CFR §70.24(a)) is not associated specifically with meeting the safety criteria prescribed in §70.61. Criticality is prevented by design "under normal and credible abnormal conditions" in the MFFF in accordance with §70.61(d) and the double contingency principle in accordance with §70.64(a)(9). Criticality alarms play no role in preventing criticality, and mitigation of events beyond the criteria of §70.61 is not required in defining items relied on for safety. Criticality monitoring and alarms are therefore not QL-1.

In particular for liquids in the MFFF, criticality is prevented typically by the geometry designed into the facility (See Table 6-1 as amended in response to Question 83). As described in the MPQAP, QL-1 SSCs are reserved for those SSCs whose failure can potentially result in an accident or which are needed to mitigate potential accident consequences, or prevent criticality. SSCs whose failure can result in a criticality accident are designated QL-1; the failure of the criticality monitors cannot result in a criticality accident.

Because the criticality monitoring and alarm system is not QL-1 does not mean it is unimportant. Such a system is a specific requirement of the regulation (in §70.24), and as an SSC that functions to further reduce worker risks below §70.61 performance requirements, it is subject to QA controls under QL-2. The CAAS is also subject to the extensive commitments made in Section 6.3.2 of the CAR, including commitment to ANSI/ANS-8.3-1997. These commitments and requirements provide reasonable assurance that the design and operation of the CAAS will meet applicable requirements.

Action:

None

238. <u>Section 15.1, pp. 15-1 thru 15-5</u>

Discuss the application and implementation of 10 CFR 21 requirements and procedures on the MOX project activities before operation, including MOX facility construction and design and MOX fuel design and qualification activities. Also explain why only IROFS SSCs and not QL-2 SSCs would be subject to 10 CFR 21 requirements.

SRP Section 15.4.3.D states that the requirements of 10 CFR 21 should be addressed by the applicant.

Response:

Question 2 of the NRC's "Request for Additional Information on the Duke Cogema Stone & Webster (DCS) Mixed Oxide Project Quality Assurance Plan, Revision 2" (NRC letter dated 6/19/01) requested the same information. See the DCS response to that question in DCS letter dated 7/18/01, DCS-NRC-000054, "Response to NRC Request for Additional Information on MOX Project Quality Assurance Plan (MPQAP) Revision 2".

Action:

Revise Section 15.1.8 of the CAR as described in the Action for QAP Question 2 in DCS letter dated 7/18/01.

239. Section 15.2, pp. 15-5 thru 15-12

Discuss how the commitment to configuration management application during design and construction for establishing and controlling the design bases includes all SSCs, not just principal SSCs and IROFS. Describe how the configuration management process functions for documenting the baseline configuration and controlling all changes and provides adequate assurance during construction, including field changes, as-built documentation, and applicant, subcontractor and supplier non-conformances.

10 CFR 70.72 requires a configuration management system to evaluate, implement and track each change to the site, structures, processes, systems, equipment, components, computer programs, and activities of personnel. The SRP Section 15.2.3.A states the construction authorization review should examine the applicant's establishment of a baseline configuration management policy applicable to all design and construction. The review should examine the applicant's establishment of a baseline configuration management policy applicable to all design and construction.

Section 15.2 of the application states that configuration management is applied to principal SSCs. The management commitments, policy directives and procedures for configuration management should be clearly specified.

Response:

Design-phase configuration management is accomplished through design control procedures which provide for configuration management of principal SSCs; the same design control procedures are used for design of non-principal SSCs as well. As part of detailed design, the Integrated Safety Analysis (ISA) will consider all aspects of design and will validate the safety basis in consideration of both principal and non-principal SSCs (principal SSCs become IROFS – or are justified as not being IROFS – as a result of the ISA process).

During the construction phase, the configuration management program is expanded to include reviews of field changes, as-built configurations, and non-conformances for impact to the design basis and the ISA.

During licensed operation, DCS will adhere to 10 CFR 70.72, which provides for evaluation, implementation, and tracking of changes to the site, structures, processes, systems, equipment, components, computer programs, and activities of personnel. These provisions include evaluation of changes to non-IROFS to ensure no inadvertent changes or impacts to IROFS occur as a result. DCS will revise Section 15.2 of the CAR to reflect that the 10 CFR 70.72 configuration management program applies to all changes.

Action:

Revise the CAR to reflect the above information