11.0 PLANT SYSTEMS

11.6 INSTRUMENTATION AND CONTROL SYSTEMS

11.6.1 CONDUCT OF REVIEW

This chapter of the revised draft Safety Evaluation Report (DSER) contains the staff's review of instrumentation and control (I&C) systems described by the applicant in Chapter 11 of the revised Construction Authorization Request (CAR). The objective of this review is to determine whether the I&C principal structures, systems, and components (PSSCs) and their design bases identified by the applicant provide reasonable assurance of protection against natural phenomena and the consequences of potential accidents. The staff evaluated the information provided by the applicant for I&C systems by reviewing Chapter 11 of the revised CAR, other sections of the revised CAR, supplementary information provided by the applicant, and relevant documents available at the applicant's offices but not submitted by the applicant. The review of I&C systems design bases and strategies was closely coordinated with the review of the electrical and I&C aspects of accident sequences described in the Safety Assessment of the Design Bases (see Chapter 5.0 of this revised DSER), and the review of other plant systems.

The staff reviewed how the I&C information in the revised CAR addresses the following regulations:

- Section 70.23(b) of 10 CFR states, as a prerequisite to construction approval, that the design bases of the PSSCs and the quality assurance program be found to provide reasonable assurance of protection against natural phenomena and the consequences of potential accidents.

- Section 70.64 of 10 CFR requires that baseline design criteria (BDC) and defense-in-depth practices be incorporated into the design of new facilities. With respect to I&C, 10 CFR 70.64(a)(10) requires that the Mixed Oxide Fuel Fabrication Facility (MFFF or the facility) design "provide for inclusion of instrument and control systems to monitor and control the behavior of items relied on for safety."

The review for this construction approval focused on the design basis of I&C systems, their components, and other related information. For each I&C system, the staff reviewed information provided by the applicant for the safety function, system description, and safety analysis. The review also encompassed proposed design basis considerations such as redundancy, independence, reliability, and quality. The staff used Chapter 11 in NUREG-1718, "Standard Review Plan for the Review of an Application for a Mixed Oxide (MOX) Fuel Fabrication Facility," as guidance in performing the review.

11.6.1.1 System Description

The facility I&C systems include the MOX processing (MP) and aqueous polishing (AP) process control, utility control, and emergency control systems.

11.6.1.1.1 Function

The I&C systems (as described in Section 11.6, "Instrumentation and Control Systems," of the revised CAR) are to monitor and control the manufacturing process systems, the plant utility systems, and the plant safety and emergency systems. Specifically, I&C systems are to monitor and control plant parameters during normal and transient conditions to ensure the quality of the produced product and ensure that limits (including safety limits) are not exceeded. They also provide control signals to plant equipment to prevent the occurrences of faulted conditions and mitigate the consequences of faulted conditions should they occur.

11.6.1.1.2 Major Components

11.6.1.1.2.1 MP and AP Process Control Systems

The MP and AP process control systems use an automated, distributed processing control system strategy with the manufacturing process translated into control algorithms for each process step. The systems include the normal, protective, and safety control subsystems which ensure the final product conforms to specifications and reduce plant waste and risk. Specifically, the normal control subsystem controls the manufacturing process, the protective control subsystem protects personnel (industrial safety) and equipment, and the safety control subsystem ensures safety limits will not be exceeded and that undesirable operational conditions are prevented or mitigated.

The process control systems are built around programmable logic controllers (PLCs) which, in turn, are built around software-controlled microprocessors. The single channels of the safety control subsystem are separate and independent from the other two control subsystems.

Any channel in the safety control subsystem in the AP or MP process control system may be designated a PSSC as a result of the applicant's facility safety analysis. The design basis for that channel of the safety control subsystem will then be as described in revised DSER Section 11.6.1.3.1 for a PSSC.

11.6.1.1.2.2 Utility Control Systems

The utility control systems also use a PLC/microprocessor-based automated, distributed processing control strategy and includes separate normal, protective, and safety control subsystems which ensure that the plant support (utility) systems operate within specifications. Specifically, the normal control subsystem controls operation of the support systems, the protective control subsystem protects personnel and equipment, and the safety control subsystem ensures that plant safety systems operate properly. The single channels of the normal and safety control subsystems are separate and independent from each other and the protective control subsystem. The safety control subsystems that are part of the utility control systems are not credited by DCS towards meeting the performance requirements of 10 CFR 70 and have not been identified as PSSCs.

11.6.1.1.2.3 Emergency Control System

The emergency control system is a PSSC and consists of manual and some automatic controls for power, ventilation, and required safety functions. Specifically, the emergency control system ensures particular plant support systems operate when needed to mitigate the consequences of hazardous occurrences. The system is a hard-wired system with no software control and is designed to continue to operate during and following specific design basis events. It is divided into two separate and independent trains, each with its separate control room.

11.6.1.1.2.4 Data Communications Networks

The data communications networks employ Ethernet technology and provide for communications among various systems and components such as normal controllers, workstations, the manufacturing management and information system (MMIS), the manufacturing status system, and the computer-aided diagnosis system. For the AP and MP process control systems, Fieldbus technology or hard-wired methods are used to link normal controllers to motor control centers and sensor/instruments. The X-terminal network (XTN) links display terminals, workstations, MMIS, manufacturing status system, and the computer-aided diagnosis system. The local industrial network (LIN) links workstations, controllers, MMIS, manufacturing status system, and the computer-aided diagnosis system. The immediate control network (ICN) links the workstations and normal controllers. Separate connections are used to connect each device to each network.

For the utility control systems, Fieldbus technology or hard-wired methods are used to link normal controllers to motor control centers (MCCs) and sensor/instruments. Dual redundant networks link the workstations and normal controllers. Separate connections are used to connect each device to each network.

11.6.1.1.2.5 Control Rooms

The facility includes various control rooms with workstations (industrial personal computers) to monitor and control the operation of the AP and MP functional units and utility system. Access to the control system data communication network is provided in the control rooms and emergency stop switches typically provide manual control capability. Human factors engineering principles are used in the design of the control rooms (see revised DSER Chapter 12). The major control rooms are discussed in the following sections.

- AP and MP Control Rooms

  The AP and MP control rooms provide central locations for monitoring, supervising, and controlling the manufacturing and processing operations. In these control rooms, operators access production control information for verification that process automation is performing satisfactorily or receive notification of a problem. Video displays of the actual functional unit conditions are provided. If an AP or MP manufacturing process functional unit is not operating, manning of the associated control room, for the particular manufacturing process steps, is not required.

  In addition to providing for the control of AP systems, the AP control room is always manned and provides for the control of the normal and safety utilities systems, the fire detection systems, and the health physics systems.

- Utilities Control Room

  In addition to the controls for the utilities systems located in the AP control room, the utilities control room provides support system monitoring and controlling capability when the controls in the AP control room for the utilities systems are unavailable. Support systems monitored and controlled from these two redundant locations include the heating, ventilation, and air-conditioning (HVAC) systems, the electrical distribution system, and other various process support systems such as the hot and chilled water system.

- Emergency Control Rooms

  Two separate emergency control rooms (Train A and Train B) each with an independent ventilation system are located in the Shipping and Receiving Building. Traditional electromechanical control devices in these control rooms are hard-wired to principal SSCs in the emergency control system. These controls have priority over the utility safety (utility backup) controls.

11.6.1.1.2.6 Sensors

The facility functional units are provided with sensors and instruments (parts of the process control systems) to monitor and measure operational conditions and parameters such as temperature, pressure, mass, component identification bar codes, machine tool and valve positions, etc. Some of the information is provided as inputs for the automatic control of actuators (fans, pumps, heaters, conveyers, etc.) and other devices which perform steps in the manufacturing process.

The utility control systems are also provided with sensors and instruments to monitor the performance of support systems such as the electrical power and HVAC systems. These sensors also provide input signals for the automatic controllers for the various utility control systems.

11.6.1.1.2.7 Controllers

The AP and MP process and the utility control systems have controllers which receive inputs from sensors and instruments. Specific controllers are discussed in the following sections.

- Normal Controllers

  PLCs provide for the control of normal operations of the functional and utility units. These normal controllers, located in rooms close to the process they control, contain communication devices and are connected to the control system networks so that data flows between the controllers and the distributed input/output (I/O), the normal controllers of other functional and utility units, the personnel and equipment protection (PEP) controllers, the safety controllers, the workstations, MMIS, and the computer-aided diagnosis system. This data communication between controllers and systems allows coordination of activities. These controllers are not PSSCs.

- Protective Controllers

  The protective controllers are dedicated controllers that protect operations personnel from injury and functional unit equipment from damage due to inappropriate operation such as overspeed, overtorque, and overtravel. These controllers are autonomous and are not connected to the control system networks. They may be PLCs or traditional electromechanical relays and are physically located in MCCs. Protective sensors are hard-wired to the controllers with output control signals hard-wired to control circuits in MCCs or power panels. Protective controllers have priority over control signals from the normal controllers and provide performance data to the normal controllers which, in turn, provide data to workstations via the ICN. Operators cannot directly access the protective controllers and cannot routinely intervene in their operation. These controllers are not PSSCs.

- Safety Controllers

  Safety controllers in the process control of the functional units serve specific and limited functions for preventing and mitigating certain accidents. Safety controllers perform specific control functions in certain utility systems in the event of loss of the normal controller. These controllers are autonomous and are not connected to the control system network. Performance data from the safety controllers is provided to the normal controllers which, in turn, provide data to workstations via the ICN. Any safety controller in the AP or MP process control system may be designated a PSSC as a result of the facility safety analysis. The design basis for that controller will then be in accordance with revised DSER Section 11.6.1.3.1.

  The safety controllers for the functional units may be PLCs or traditional relays, are physically located in rooms separate from the normal controllers, and are hard-wired to the sensors and actuator control circuits in MCC or power distribution panels. The control signals from the safety controllers have priority over signals from the normal controllers and if a safety controller does not detect appropriate functional unit conditions, it will block commands issued by the normal controllers. Operators cannot directly access the safety controllers and cannot routinely intervene in their operation with the exception of the scrap jar isotopic concentration data which is manually loaded into the safety controllers.

  Upon receipt of a fire condition signal from the facility fire detection system, fire safety controllers direct the normal controllers to immediately close the fire doors. Following a delay, the fire safety controller will close the fire doors if the normal controllers fail to take action.

  Safety controllers in selected utility systems provide backup monitoring and control capability if the normal control systems are unavailable. They are also installed in separate locations from the normal controllers and are hard-wired to dedicated workstations located in the alternate utilities control room. Safety controllers in the utility control system have not been identified as PSSCs.

- Emergency Controllers

  The facility emergency controllers in the emergency control system are traditional relay logic circuits with control switches located on emergency control panels in the emergency control rooms. Inputs to emergency controllers from the sensors and outputs from the controllers to MCCs are hard-wired. The emergency controllers provide manual control for selected systems. These controllers are PSSCs.

11.6.1.1.2.8 MMIS

The MMIS is a realtime system that tracks the product inventory and maintains/updates the manufacturing status system database files as the product moves through the manufacturing process. It tracks quantities of product that are allowed in any area at a given time and authorizes the movement of product into or out of a functional unit. MMIS also is a server for the XTN.

11.6.1.1.2.9 Manufacturing Status System

The manufacturing status system is identical to MMIS and maintains a realtime copy of the MMIS database. The system is used to sort, analyze, and report on data collected by MMIS.

11.6.1.1.2.10 Computer-Aided Diagnosis System

The computer-aided diagnosis system monitors the operation of the normal controllers for the function units and the ICN. The system is independent from the controllers and has its own software. It provides a primary diagnostic capability when there is a problem with the production process and works with the software used in the PLCs to determine the state of the PLC when the problem occurred.

11.6.1.1.2.11 Process Computers

Process computers are dedicated microprocessor-based computers that control and handle data for the more complex process measurement systems such as the laser optical micrometer. These computers operate the measurement systems, provide data signal conditioning, and send data to the PLCs controlling the associated functional unit.

11.6.1.1.2.12 Seismic Monitoring System

The seismic monitoring system provides data for the evaluation of the confinement structure and other PSSCs and automatically shuts down the AP and MP processes during a high seismic event.

11.6.1.2 System Interfaces

The facility I&C systems are primarily electronic systems that interface with mechanical, electrical, and process systems. The system provides signals to control electromechanical and pneumatic actuators and data signals for information display, processing, and storage. The control systems and its associated components, such as electromechanical actuators, are supplied electrical power by the facility electrical systems. The pneumatic actuators are provided air by either the instrument air or plant air systems. The various control rooms provide the primary human-system interface for all the facility systems. Environmental conditions for proper operation of the I&C systems are maintained by the HVAC systems and protection against fires is provided by the fire protection systems.

11.6.1.3 Design Bases of the PSSCs and Baseline Design Criteria

For design basis requirements, the instrumentation and control systems are to be available and reliable for normal operation and safe shutdown and monitoring (see revised DSER Section 11.6.1.1.1 herein for a discussion of the function performed by the I&C systems.). With respect to I&C, 10 CFR 70.64(a)(10) requires that the facility design "provide for inclusion of instrument and control systems to monitor and control behavior of items relied on for safety." The I&C systems designated as PSSCs should remain functional when subjected to severe natural phenomena, environmental and dynamic effects, consistent with the baseline design criteria in 10 CFR 70.64(a)(2) and (a)(4), respectively and be adequately protected from fires per 10 CFR 70.64(a)(3). Additionally, the I&C systems must support continued operation of essential utility services, consistent with the baseline design criterion in 10 CFR 70.64(a)(7).

Pursuant to 10 CFR 70.64(b), the I&C systems should be designed using defense-in-depth practices, with a preference engineered controls over administrative controls.

To ensure that the design basis requirements and the baseline design criteria are met, DCS has committed to specific industry standards and staff guidance as discussed in the following section.

11.6.1.3.1 I&C Systems (PSSCs)

The I&C systems identified by DCS as PSSCs are the emergency control system and the AP and MP safety control subsystems (Reference 11.6.3.46). These PSSCs will be designed with provisions for periodic testing, redundancy, independence, no single failure vulnerability, fail safe failure mode, proper instrument spans/setpoints/control ranges, status monitoring, and qualification for natural phenomena and environmental and dynamic effects (see revised DSER Section 11.11). Additionally, these systems will be designed using guidance (to the extent described in the revised CAR and DCS letters dated August 31, 2001, December 5, 2001, January 7, 2002, November 22, 2002, and February 11, 2003 (References 11.6.3.4, 11.6.3.5, 11.6.3.6, 11.6.3.7 and 11.6.3.8) from the following:

- For overall system design (including seismic monitoring and trip system):

  Institute of Electrical and Electronics Engineers (IEEE). IEEE Std 603-1998, “IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations.”

- For single failure:

  Institute of Electrical and Electronics Engineers (IEEE). IEEE Std 379-1994, “IEEE Standard Application of the Single Failure Criterion to Nuclear Power Generation Station Safety Systems.”

- For software programmable electronic systems:

  Electric Power Research Institute (EPRI). EPRI Topical Report TR-106439, “Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications.” October 1996.

  International Electrotechnical Commission (IEC). IEC 61131-3 (1993-03), “Programmable Controllers - Part 3: Programming Languages.”

  Institute of Electrical and Electronics Engineers (IEEE). IEEE Std 7-4.3.2-1993, “IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations.”

  ——————. IEEE Std 730-1998, ”Software Quality Assurance Plans.”

  ——————. IEEE Std 828-1998, “IEEE Standard for Software Configuration Management Plans.”

  ——————. IEEE Std 830-1998, “IEEE Standard Recommended Practice for Software Requirements Specifications.”

  ——————. IEEE Std 1012-1998, “IEEE Standard for the Software Verification and Validation.”

  ——————. IEEE Std 1028-1997, “IEEE Standard for Software Reviews.”

  ——————. IEEE Guide 1042-1987, ”Software Configuration Management.”

——————. IEEE Std 1074-1997, “IEEE Standard for Developing Software Life Cycle Processes.”

——————. IEEE Std 1228-1994, “IEEE Standard for Software Safety Plans.”

Nuclear Regulatory Commission (U.S.) (NRC). NUREG/CR-6090, “The Programmable Logic Controller and Its Application in Nuclear Power Plants.” NRC: Washington, D.C. February 1999.

——————. NUREG/CR-6463, “Review Guidelines on Software Languages for Use in Nuclear Power Plant Safety Systems.” NRC: Washington, D.C. June 1996.

——————. Regulatory Guide 1.168, “Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants.” NRC: Washington, D.C. September 1997.

——————. Regulatory Guide 1.169, Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants.” NRC: Washington, D.C. September 1997.

——————. Regulatory Guide 1.172, “Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants.” NRC: Washington, D.C. September 1997.

——————. Regulatory Guide 1.173, “Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants.” NRC: Washington, D.C. September 1997.

——————. Safety Evaluation by the Office of Nuclear Reactor Regulation, “EPRI Topical Report TR-106439.” May 1997.

- For electrical independence and separation:

Institute of Electrical and Electronics Engineers (IEEE). IEEE Std 384-1992, “Standard Criteria for Independence of Class 1E Equipment and Circuits.”

Nuclear Regulatory Commission (U.S.) (NRC). NUREG-800, Standard Review Plan, Branch Technical Position HICB-11, “Guidance on the Application and Qualification of Isolation Devices.” NRC: Washington, D.C.

——————. Regulatory Guide 1.75, Revision 2, “Physical Independence of Electric Systems.” NRC: Washington, D.C. September 1978.

- For equipment seismic qualification:

Institute of Electrical and Electronics Engineers (IEEE). IEEE Std 344-1987, “IEEE Recommended Practices for Seismic Qualification of Class 1E Equipment for Nuclear Generating Stations.”

Nuclear Regulatory Commission (U.S.)(NRC). Regulatory Guide 1.100, Revision 2, “Seismic Qualification of Electric and Mechanical Equipment for Nuclear Power Plants.” NRC: Washington, D.C. June 1988.

- For setpoints:

  American National Standards Institute/Instrument Society of American (ANSI/ISA). ANSI/ISA-67.04.01-2000, “Setpoints for Nuclear Safety-Related Instrumentation.”

  Nuclear Regulatory Commission (U.S.) (NRC). Regulatory Guide 1.105, Revision 3, “Setpoints for Safety-Related Instrumentation.” NRC: Washington, D.C.

- For human-system interface:

  Institute of Electrical and Electronics Engineers (IEEE). IEEE Std 1023-1988. “IEEE Guide for the Application of Human Factors Engineering to Systems, Equipment, and Facilities of Nuclear Power Generating Stations.”

  Nuclear Regulatory Commission (U.S.) (NRC). NUREG-0700, Human System Design Review Guidelines. NRC: Washington, D.C.

- For the seismic monitoring and trip system (recording function):

  Nuclear Regulatory Commission (U.S.) (NRC). Regulatory Guide 3.17-1974, “Earthquake Instrumentation for Fuel Reprocessing Plants.”

- For periodic testing:

  Institute of Electrical and Electronics Engineers (IEEE). IEEE Std 338-1987, “IEEE Standard Criteria for Periodic Testing of Nuclear Power Generating Station Class 1E Power and Protection Systems.”

  Nuclear Regulatory Commission (U.S.) (NRC). NUREG-0800, Standard Review Plan, Branch Technical Position HICB-17, “Guidance on Self-Test and Surveillance Test Provisions.” NRC: Washington, D.C.

  ——————. Regulatory Guide 1.118, Revision 3, “Periodic Testing of Electric Power and Protection Systems.” NRC: Washington, D.C.

- For reduction of electromagnetic and radio frequency interference:

  Institute of Electrical and Electronics Engineers (IEEE). IEEE Std 518-1982, “IEEE Guide for the Installation of Electrical Equipment to Minimize Electrical Noise Inputs to Controllers from External Sources.”

  ——————. IEEE Std 1050-1996, “Guide for Instrumentation and Control Equipment Grounding in Generating Stations.”

  Nuclear Regulatory Commission (U.S.) (NRC). Regulatory Guide 1.180, “Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems.” NRC: Washington, D.C. January 2000.

- For design of data communications networks:

  American National Standards Institute/Institute of Electrical and Electronics Engineers (ANSI/IEEE). ANSI/IEEE 802.3 Standards Series, “IEEE Standards for Local Area

Networks: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications."

- For design of combustible gas detectors:

  Instrument Society of America (ISA). ISA-S12.13-Part 1-1995, "Performance Requirements, Combustible Gas Detectors."

  —————. ISA RP12.13-Part II-1987, "Installation, Operation, and Maintenance of Combustible Gas Detection Instruments."

In Section 5.5.5 of the revised CAR, the applicant describes its general design philosophy used in formulating the preliminary design of the facility. Pursuant to 10 CFR 70.64(b), in order to ensure that engineered controls are relied upon over administrative controls, to the extent practicable, DCS has established a hierarchy of controls. In further adherence to 10 CFR 70.64(b), DCS states that it has incorporated defense-in-depth practices in its preliminary facility design. Defense-in-depth is defined in the 10 CFR 70.64 footnote. In Section 5.5.5.2 of the revised CAR, DCS states that it has incorporated defense-in-depth practices through use of the single failure criterion. Under this criterion, PSSCs are required to be capable of carrying out their functions in the event that any single active component fails, whether such failure occurs within the applicable system, or in an associated system that supports the components's operation.

Accordingly, the facility I&C systems should be designed using defense-in-depth practices using the single failure criterion including redundancy, independence, separation, and fail safe for the I&C systems identified as PSSCs through use of the industry standards listed above. As an example, the emergency control system is designed with redundant, separate, and independent trains with fail safe failure modes (See revised DSER Section 11.6.1.1.2.3).

11.6.2 EVALUATION FINDINGS

In Section 11.6.7 of the revised CAR, DCS provided design basis information for I&C systems that it identified as PSSCs for the facility. Based on the staff's review of the revised CAR and supporting information provided by the applicant and the applicant's commitments to the industry standards and guidance discussed in the sections above for I&C systems, the staff finds that DCS has met the BDC set forth in 10 CFR 70.64(a)(10). The staff concludes, pursuant to 10 CFR 70.23(b), that the design bases of the PSSCs evaluated in this revised DSER section will provide reasonable assurance of protection against natural phenomena and the consequences of potential accidents. The staff further concludes, from its review of the revised CAR and supporting information submitted by DCS, that the preliminary design of the facility I&C systems meet the defense-in-depth provisions and the preference for engineered controls over administrative controls as stated in 10 CFR 70.64(b).

11.6.3 REFERENCES

11.6.3.1 American National Standards Institute/Instrument Society of American (ANSI/ISA). 67.04.01-2000, "Setpoints for Nuclear Safety-Related Instrumentation." ANSI/ISA: Research Triangle Park, North Carolina, 2000.

11.6.3.2 American National Standards Institute/Institute of Electrical and Electronics Engineers (ANSI/IEEE). 802.3 Standards Series, "IEEE Standards for Local Area Networks: Carrier Sense Multiple Access with Collision Detection (CSMA/CD)

Access Method and Physical Layer Specifications." ANSI/IEEE: New York, New York, 2000

11.6.3.3 Electric Power Research Institute (EPRI). Topical Report TR-106439, "Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications." EPRI: Palo Alto, California, October 1996.

11.6.3.4 Hastings, P., Duke Cogema Stone & Webster, letter to U.S. Nuclear Regulatory Commission, RE Response to Request for Additional Information (DCS-NRC-000059), August 31, 2001.

11.6.3.5 Hastings, P., Duke Cogema Stone & Webster, letter to U.S. Nuclear Regulatory Commission, RE Clarification of Responses to NRC Request for Additional Information (DCS–NRC–000074), December 5, 2001.

11.6.3.6 Hastings, P., Duke Cogema Stone & Webster, letter to U.S. Nuclear Regulatory Commission, RE Clarification of Responses to NRC Request for Additional Information, January 7, 2002.

11.6.3.7 Hastings, P., Duke Cogema Stone & Webster, letter to U.S. Nuclear Regulatory Commission, RE Requests for Additional Information, Clarifications, and Open Item Mapping into the Construction Authorization Request Revision (DCS-NRC-000120), November 22, 2002.

11.3.6.8 Hastings, P., Duke Cogema Stone & Webster, letter to U.S. Nuclear Regulatory Commission, RE Responses to Site Description, Instrumentation, and Criticality Open Items/Additional NRC Questions on Construction Authorization Request (CAR) Revision, February 11, 2003.

11.6.3.9 Institute of Electrical and Electronics Engineers (IEEE). Std 7-4.3.2-1993, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations." IEEE: New York, New York, 1993.

11.6.3.10 ——————. Std 338-1987, "IEEE Standard Criteria for Periodic Testing of Nuclear Power Generating Station Class 1E Power and Protection Systems." IEEE: New York, New York, 1987.

11.6.3.11 ——————. Std 344-1987, "IEEE Recommended Practices for Seismic Qualification of Class 1E Equipment for Nuclear Generating Stations." IEEE: New York, New York, 1987.

11.6.3.12 ——————. Std 379-1994, "IEEE Standard Application of the Single Failure Criterion to Nuclear Power Generation Station Safety Systems." IEEE: New York, New York, 1994.

11.6.3.13 ——————. Std 384-1992, "Standard Criteria for Independence of Class 1E Equipment and Circuits." IEEE: New York, New York, 1992.

11.6.3.14 ——————. Std 518-1982, "IEEE Guide for the Installation of Electrical Equipment to Minimize Electrical Noise Inputs to Controllers from External Sources." IEEE: New York, New York, 1982.

11.6.3.15 ——————. Std 603-1998, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations." IEEE: New York, New York, 1998.

11.6.3.16 ——————. Std 730-1998, "Software Quality Assurance Plans." IEEE: New York, New York, 1998.

11.6.3.17 ——————. Std 828-1998, "IEEE Standard for Software Configuration Management Plans." IEEE: New York, New York, 1998.

11.6.3.18 ——————. Std 830-1998, "IEEE Standard Recommended Practice for Software Requirements Specifications." IEEE: New York, New York, 1998.

11.6.3.19 ——————. Std 1012-1998, "IEEE Standard for the Software Verification and Validation." IEEE: New York, New York, 1998.

11.6.3.20 ——————. Std 1023-1988. "IEEE Guide for the Application of Human Factors Engineering to Systems, Equipment, and Facilities of Nuclear Power Generating Stations." IEEE: New York, New York, 1998.

11.6.3.21 ——————. Std 1028-1997, "IEEE Standard for Software Reviews." IEEE: New York, New York, 1997.

11.6.3.22 ——————. Guide 1042-1987, "Software Configuration Management." IEEE: New York, New York, 1987.

11.6.3.23 ——————. Std 1050-1996, "Guide for Instrumentation and Control Equipment Grounding in Generating Stations." IEEE: New York, New York, 1996.

11.6.3.24 ——————. Std 1074-1997, "IEEE Standard for Developing Software Life Cycle Processes." IEEE: New York, New York, 1997.

11.6.3.25 ——————. Std 1228-1994, "IEEE Standard for Software Safety Plans." IEEE: New York, New York, 1994.

11.6.3.26 Instrument Society of America (ISA). ISA-S12.13-Part 1-1995, "Performance Requirements, Combustible Gas Detectors."

11.6.3.27 ——————. ISA RP12.13-Part II-1987, "Installation, Operation, and Maintenance of Combustible Gas Detection Instruments."

11.6.3.28 International Electrotechnical Commission (IEC). 61131-3 (1993-03), "Programmable Controllers - Part 3: Programming Languages." IEC: Geneva, Switzerland, 1993.

11.6.3.29 Nuclear Regulatory Commission (U.S.) (NRC). NUREG-0700, Human System Design Review Guidelines. NRC: Washington, D.C.

11.6.3.30 ——————. NUREG-800, Standard Review Plan, Branch Technical Position HICB-11, "Guidance on the Application and Qualification of Isolation Devices." NRC: Washington, D.C.

11.6.3.31 —————. NUREG-0800, Standard Review Plan, Branch Technical Position HICB-17, “Guidance on Self-Test and Surveillance Test Provisions.” NRC: Washington, D.C.

11.6.3.32 —————. NUREG/CR-6090, ”The Programmable Logic Controller and Its Application in Nuclear Power Plants.” NRC: Washington, D.C. February 1999.

11.6.3.33 —————. NUREG/CR-6463, “Review Guidelines on Software Languages for Use in Nuclear Power Plant Safety Systems.” NRC: Washington, D.C. June 1996.

11.6.3.34 —————. NUREG/CR-6597, “Results and Insights on the Impact of Smoke on Digital Instrumentation and Control.” NRC: Washington, D.C. January 2001.

11.6.3.35 —————. Regulatory Guide 1.75, Revision 2, “Physical Independence of Electric Systems.” NRC: Washington, D.C. September 1978.

11.6.3.36 —————. Regulatory Guide 1.100, Revision 2, “Seismic Qualification of Electric and Mechanical Equipment for Nuclear Power Plants.” NRC: Washington, D.C. June 1988.

11.6.3.37 —————. Regulatory Guide 1.105, Revision 3, “Setpoints for Safety-Related Instrumentation.” NRC: Washington, D.C.

11.6.3.38 —————. Regulatory Guide 1.118, Revision 3, “Periodic Testing of Electric Power and Protection Systems.” NRC: Washington, D.C.

11.6.3.39 —————. Regulatory Guide 1.168, “Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants.” NRC: Washington, D.C. September 1997.

11.6.3.40 —————. Regulatory Guide 1.169, Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants.” NRC: Washington, D.C. September 1997.

11.6.3.41 —————. Regulatory Guide 1.172, “Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants.” NRC: Washington, D.C. September 1997.

11.6.3.42 —————. Regulatory Guide 1.173, “Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants.” NRC: Washington, D.C. September 1997.

11.6.3.43 —————. Regulatory Guide 1.180, “Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems.” NRC: Washington, D.C. January 2000.

11.6.3.44 —————. Regulatory Guide 3.17-1974, “Earthquake Instrumentation for Fuel Reprocessing Plants.”

11.6.3.45 —————. Safety Evaluation by the Office of Nuclear Reactor Regulation, “EPRI Topical Report TR-106439.” May 1997.

11.6.3.46 Ihde, R., Duke Cogema Stone & Webster, letter to U.S. Nuclear Regulatory Commission, RE Mixed Oxide Fuel Fabrication Facility Construction Authorization Request Revision (DCS-NRC-000114), October 31, 2002.