



UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D.C. 20555-0001

SAFETY EVALUATION BY THE OFFICE OF NUCLEAR REACTOR REGULATION

RELATED TO AMENDMENT NO. 26 TO

RENEWED FACILITY OPERATING LICENSE NO. R-84

ARMED FORCES RADIOBIOLOGY RESEARCH INSTITUTE

ARMED FORCES RADIOBIOLOGY RESEARCH INSTITUTE REACTOR FACILITY

DOCKET NO. 50-170

1.0 INTRODUCTION

By application dated November 10, 2020 (Agencywide Documents Access and Management System (ADAMS) Package Accession No. ML20318A338 (Reference (Ref.) 1), as supplemented by letters dated February 5, 2021 (ADAMS Accession No. ML21036A297) (Ref. 2), February 11, 2021 (ADAMS Accession No. ML21042B841) (Ref. 3), October 28, 2021 (ADAMS Accession No. ML21302A096) (Ref. 4), November 8, 2021 (ADAMS Accession No. ML21316A032) (Ref. 17), January 7, 2022 (ADAMS Accession No. ML22007A263) (Ref. 16), April 4, 2022 (ADAMS Accession No. ML22096A279) (Ref. 18), and April 28, 2022 (ADAMS Accession No. ML22118A867) (Ref. 21), the Armed Forces Radiobiology Research Institute (the licensee, AFRRRI) applied for an amendment to Renewed Facility Operating License No. R-84 for the AFRRRI Training, Research, Isotopes, General Atomics (TRIGA)-Mark F tank-type nuclear reactor facility (the facility). The submitted request would upgrade the instrumentation and control (I&C) systems for the facility by replacing them with new analog I&C or digital instrumentation and control (DI&C) systems. Additionally, the licensee requested changes to the facility's technical specifications (TSs) for two limiting conditions for operation (LCOs): TS 3.2.2, "Reactor Safety Systems," Table 2, "Minimum Reactor Safety System Scrams," watchdog timer circuits and alternating current (AC) power loss and TS 3.2.2, Table 3, "Minimum Reactor Safety System Interlocks," and two surveillance requirements (SRs): TS 4.2.2, "Reactor Safety Systems," Specifications b., c., and e., and TS 4.2.4. "Facility Interlock System," Specification b.

The proposed I&C systems for the facility consist of hybrid analog and digital systems to monitor, protect, and control the reactor. The proposed I&C systems include a hardwired reactor protection system (RPS) with dedicated displays and controls so that safe operation and monitoring of the reactor is not affected if the digital systems become unavailable. Components of the I&C systems will be installed in the data acquisition cabinet (DAC). The reactor will be operated from the control system console (CSC) located in the control room. Section 3.0 of this safety evaluation (SE) provides the U.S. Nuclear Regulatory Commission (NRC, the Commission) staff's technical evaluation of these systems.

In particular, the licensee proposes the following TS changes:

- (1) Revise TS 3.2.2, Table 2 to add a second watchdog timer circuit, change the name of the watchdog timer circuits from “DAC to CSC” to “UIT and CCS,” and add an AC power loss scram circuit.
- (2) Revise TS 3.2.2, Table 3 to replace the term “operational channel” with “Linear Power Channel” for the NMP-1000 and with “Log Power Channel” for the NLW-1000, and change the units for the low source interlock setpoint from counts per second (cps) to watts.
- (3) Revise TS 4.2.2, Specification b. to delete one instance of the repeated words “of each” and to specify that the channels to be tested are the reactor safety system channels as specified in TS 3.2.2, Table 2 and Table 3, except for the exposure room emergency stop and AC power loss scrams.
- (4) Revise TS 4.2.2, Specification c. to add that channel calibration shall include annual verification of the setpoints for the high voltage loss to safety channel scrams and to remove “NM1000.”
- (5) Revise TS 4.2.2, Specification e. to require that the exposure room emergency stop and AC power loss scrams be tested annually.
- (6) Revise TS 4.2.4, Specification b. to add the exception that the core dolly cannot be moved in region 2 with the lead doors closed except during the use of the core dolly interlock override switch.

The NRC staff completed a regulatory audit (Audit) of the facility on January 27, 2022; performance of this Audit was in accordance with the audit plan (Ref. 19). The Audit Report, dated March 29, 2022 (ADAMS Accession No. ML22067A246) (Ref. 5) describes the topics examined during the Audit. As a result of the Audit, the licensee supplemented its application with Supplement 2 (Ref. 4), which included the license amendment request (LAR), Revision (Rev. 1), LAR Supplement, Rev. 1, and safety analysis report (SAR), Rev. 1, and submissions on April 4 and 28, 2022.

2.0 REGULATORY EVALUATION

The NRC staff reviewed the LAR and evaluated the proposed changes to the TSs based on the following regulations and guidance:

- Part 50, “Domestic Licensing of Production and Utilization Facilities,” of Title 10 of the *Code of Federal Regulations* (10 CFR), which provides the regulatory requirements for licensing of non-power reactors.
- Section 50.34(a)(7) of 10 CFR, which requires the applicant to describe the quality assurance (QA) program for the design, fabrication, construction, and testing of the structures, systems, and components of the facility and 10 CFR 50.34(b)(6)(ii), which requires that a final safety analysis report include the managerial and administrative controls to be used to assure safe operation.
- Section 50.34(a)(3)(i) of 10 CFR, which requires the applicant to describe the principal design criteria for the facility.

- Section 50.34(a)(3)(ii) of 10 CFR, which requires the applicant to describe the design bases and the relation of the design bases to the principal design criteria.
- Section 50.34(a)(4) of 10 CFR, which requires a preliminary analysis and evaluation of the design and performance of structures, systems, and components of the facility with the objective of assessing the risk to public health and safety resulting from operation of the facility and including determination of the margins of safety during normal operations and transient conditions anticipated during the life of the facility, and the adequacy of structures, systems, and components provided for the prevention of accidents and the mitigation of the consequences of accidents.
- Section 50.34(b)(2) of 10 CFR, which requires a description and analysis of the structures, systems, and components of the facility, with emphasis upon performance requirements, the bases, with technical justification therefor, upon which such requirements have been established, and the evaluations required to show that safety functions will be accomplished. The description shall be sufficient to permit understanding of the system designs and their relationship to safety evaluations.
- Section 50.34(b)(2)(i) of 10 CFR, which requires that such items as the “instrumentation and control systems” and “electrical systems” be discussed insofar as they are pertinent.
- Section 50.34(b)(4) of 10 CFR, which requires a final analysis and evaluation of the design and performance of structures, systems, and components with the objective stated in 10 CFR 50.34(a)(4) and considering any pertinent information developed since the submittal of the preliminary safety analysis report.
- Section 50.36(a)(1) of 10 CFR, which requires that each applicant for a license authorizing operation of a production or utilization facility include in the application proposed technical specifications and a summary statement of the bases or reasons for such specifications, other than those covering administrative controls; the bases shall be included in the application, but shall not become part of the technical specifications.
- Section 50.36(b) of 10 CFR, which requires that the TSs be derived from the analyses and evaluation included in the safety analysis report.
- Section 50.36(c) of 10 CFR, which requires the TSs to include, in part:
 - LCOs, which are the lowest functional capability or performance levels of equipment required for safe operation of the facility (10 CFR 50.36(c)(2)).
 - SRs relating to test, calibration, or inspection to assure that the necessary quality of systems and components is maintained, that facility operation will be within safety limits, and that the LCOs will be met (10 CFR 50.36(c)(3)).
- NUREG-1537, Parts 1 and 2, “Guidelines for Preparing and Reviewing Applications for the Licensing of Non-Power Reactors,” “Format and Content,” and “Standard Review Plan and Acceptance Criteria,” respectively (Ref. 6), provide guidance to the NRC staff for performing safety reviews of applications to construct, modify, or operate a non-power reactor. The NRC staff used NUREG-1537, Part 2 as guidance and acceptance criteria for the review of the application to upgrade the AFRRRI facility’s I&C systems in

order to verify compliance with the applicable regulatory requirements listed above. NUREG-1537, Parts 1 and 2 reference additional guidance, including:

- Regulatory Guide 1.152, Rev. 1, "Criteria for Digital Computers in Safety Systems of Nuclear Power Plants," dated 1996 (Ref. 13), which, to the extent applicable to research reactors, provides guidance for the use of digital computers in nuclear safety systems including computer hardware, software, firmware, and interfaces and in which the NRC staff endorses the use of Institute of Electrical and Electronics Engineers (IEEE) standard IEEE 7-4.3.2-1993 (Ref. 11).
- Regulatory Guide 2.5, Rev. 0, "Quality Assurance Program Requirements for Research Reactors," dated 1977 (Ref. 12), which describes a method acceptable to the NRC staff for complying with the regulations for quality assurance program requirements for research reactors and in which the NRC staff endorses the use of American National Standards Institute/American Nuclear Society (ANSI/ANS) 15.8-1976.
- ANSI/ANS-15.1-1990, "The Development of Technical Specifications for Research Reactors" (Ref. 7), which provides guidance that identifies and establishes the content of TSs for research reactors.
- ANSI/ANS-15.8-1995, "Quality Assurance Program Requirements for Research Reactors" (Ref. 8), which provides the general requirements for establishing and executing a quality assurance program for the design, construction, testing, modification, and maintenance of research reactors.
- ANSI/ANS-15.15-1978, "Criteria for the Reactor Safety Systems of Research Reactors" (Ref. 9), which provides the criteria for establishing appropriate specific design requirements for the reactor safety system of an individual research reactor.
- ANSI/ANS-10.4-1987, "Guidelines for the Verification and Validation of Scientific and Engineering Computer Programs for the Nuclear Industry" (Ref. 10), which provides guidelines for the verification and validation (V&V) of scientific and engineering computer programs developed for use by the nuclear industry.
- IEEE 7-4.3.2-1993, "IEEE Standard Criteria for Digital Computers Systems in Safety Systems of Nuclear Power Generating Stations" (Ref. 11), which, to the extent applicable to research reactors, provides guidance to establish minimum functional and design requirements for computers used as components of a nuclear safety system.

3.0 TECHNICAL EVALUATION

AFRRI is the licensee for a TRIGA reactor licensed for steady-state thermal power levels up to and including 1.1 megawatts thermal (MWt) and short-duration power pulses with reactivity insertions up to the TS 3.1.2, "Pulse Mode Operation," limit of 3.50 (2.45 percent $\Delta k/k$ (% $\Delta k/k$, excess reactivity in percent)). The primary mission of the AFRRI TRIGA reactor is to conduct scientific research in the field of radiobiology and related radiation research in support of the U.S. Department of Defense (DOD).

The initial license, granted in June 1962 by the Atomic Energy Commission, was renewed in November 2016 (ADAMS Accession No. ML16278A347).

The AFRRI reactor is a heterogeneous pool-type reactor cooled by the natural convection of light water. The reactor is moderated primarily by zirconium hydride and, to a lesser extent, by the cooling water and is reflected by pool water and a graphite moderator as end plugs of each fuel element. The core and control system are suspended on a bridge mounted on rails that allows the core to be moved across the pool to face exposure rooms (ERs) on both sides of the tank. The revised SAR, Rev. 1, Section 7.1 (Ref. 4) describes the reactor instrumentation as consisting of three fission chambers, a compensated ionization chamber, an uncompensated ionization chamber, a Cherenkov detector, and fuel elements with integrated thermocouples. The reactor instrumentation is evaluated in Section 3.3 of this SE. The control room is located adjacent to the reactor room to allow the operator to observe the reactor room, the reactor pool, and the top structures of the reactor through a large window. The reactor is located within a reinforced concrete biological shield structure.

The AFRRI reactor serves as a source of both gamma and neutron radiation for research and radioisotope production. The revised LAR, Rev. 1 (Ref. 4) describes the irradiation facilities. The reactor includes two ERs located at opposite ends of the reactor tank. A portion of the reactor tank extends into each ER. The facility also includes an in-core experiment tube (CET). The CET is primarily used for the production of radioisotopes and the activation of samples for subsequent analysis.

In 1990, the licensee submitted an LAR to install a microprocessor-based I&C system. License Amendment No. 19, dated July 23, 1990, approved the installation of the microprocessor-based I&C system (Ref. 14).

The AFRRI fuel temperature safety limit (SL) (TS 2.1) is specified not to exceed 1,000 degrees Celsius ($^{\circ}\text{C}$) (1,832 (degrees Fahrenheit ($^{\circ}\text{F}$))) under any mode of operation. To ensure that this SL is not exceeded, the limiting safety system setting (LSSS) (TS 2.2) is established for steady-state or pulse operation for fuel temperature to be less than or equal to 600°C (1,112 $^{\circ}\text{F}$), as measured in the instrumented fuel elements (IFEs) located in specific locations in the core.

3.1. Instrumentation and Control Systems

The proposed I&C systems for the AFRRI reactor consist of a combination of both analog and digital equipment to monitor, control, and protect as follows:

- complete information on the status of the reactor and reactor-related systems
- a means for manually withdrawing or inserting control rods
- automatic control of reactor power level
- automatic scrams in response to overpower, loss of detector high voltage, or high fuel temperature conditions
- monitoring of radiation and airborne radioactivity levels

In the figure in Ref. 21, reproduced as Figure 1 below, the simplified block diagram illustrates the proposed I&C system for the AFRRI reactor. This figure identifies components that are retained and unchanged and new components that replace obsolete items.

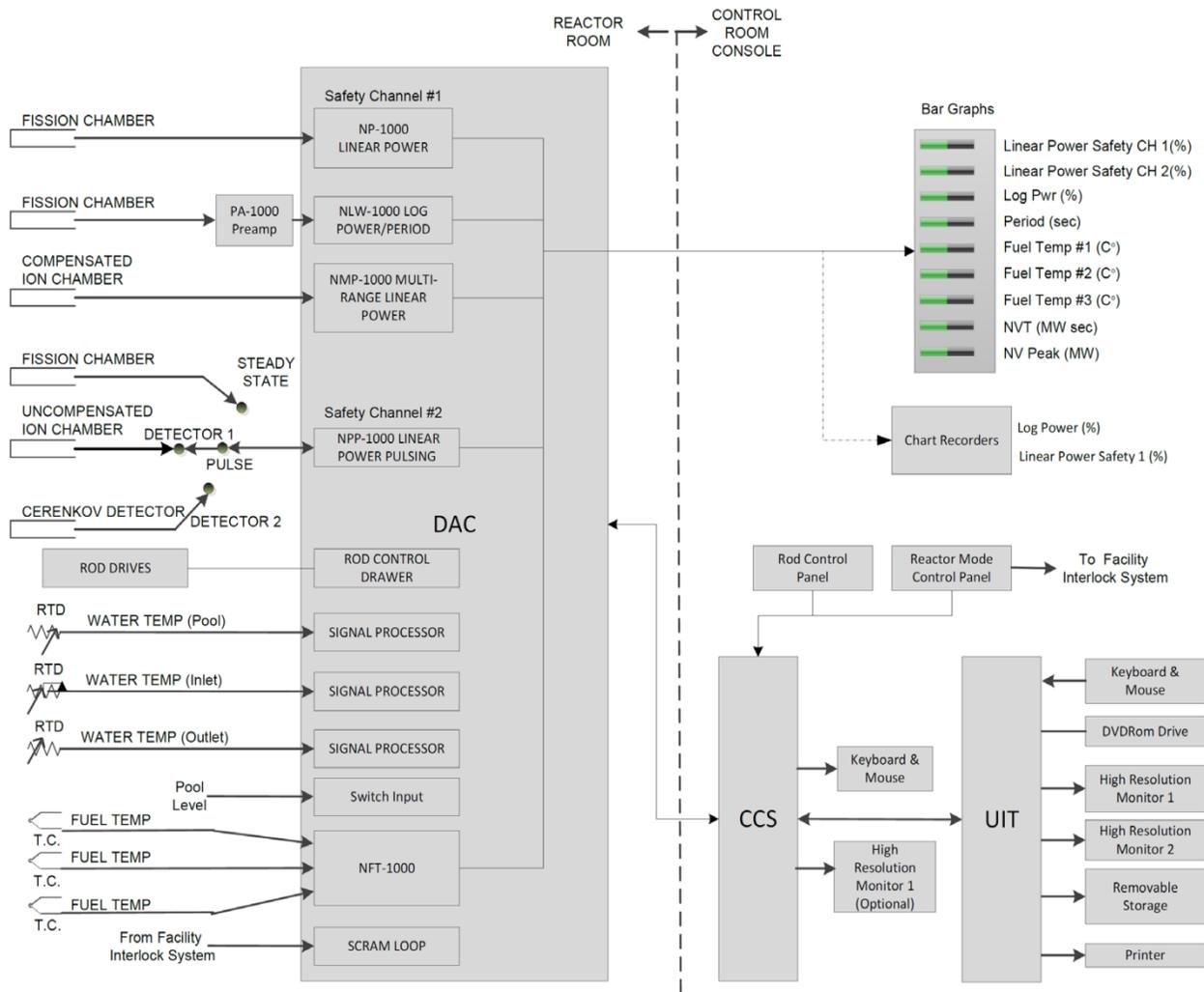


Figure 1 – Diagram of Major Components for the AFRR Reactor Instrumentation and Control System

The I&C system includes the following systems. These systems and its subsystems are described and evaluated in the listed sections.

- Data Acquisition Cabinet (DAC), which houses the nuclear instrument (NI) modules, the drivers for the control rod drives (CRDs), and equipment to process analog and digital inputs (Section 3.2 of this SE).
- Reactor Instrumentation, which includes the neutron monitoring system, consists of the following: NP-1000, NPP-1000, NMP-1000, NLW-1000, and NFT-1000 modules (Section 3.3 of this SE).
- Reactor Control System, which includes CRDs, automatic control, and reactor interlocks (Section 3.4 of this SE).
- Facility Interlock System (FIS), which includes interlocks to eliminate the possibility of accidental radiation exposure of personnel working in the ERs (Section 3.5 of this SE).

- Reactor Protection System, which includes the scram logic circuitry, rod withdrawal prevention, facility interlocks, and lead shield door control (Section 3.6 of this SE).
- Control System Console (CSC), which includes indicators, annunciators, and monitors to monitor and control the reactor (Section 3.7 of this SE).
- Process instrumentation, which includes pool water level, primary water temperature, and primary water conductivity (Section 3.8 of this SE).
- Radiation monitoring system, which includes radiation air monitors (RAMs), continuous air monitors (CAMs), and gas stack monitor. The licensee stated that the RAMS, CAMS, and gas stack monitor instrumentation are not modified as part of the LAR. Therefore, the NRC staff did not reevaluate the existing radiation monitoring system.

The AFRRRI reactor design basis SL is fuel temperature of 1,000°C. Design features, operating limits, and automatic scrams help ensure that this SL is not exceeded.

The AFRRRI reactor can be operated at steady-state power level or in pulse mode. During steady-state, the power level can reach the license level of 1.1 MWt. During a pulse, rapid positive reactivity insertion causes a prompt increase in reactor power level and a corresponding increase in fuel temperature. The negative temperature coefficient of the fuel limits the magnitude of the peak power. When the pulse is initiated, the movement of the transient rod determines the amount of reactivity inserted. Peak power resulting from pulse reactivity insertion is monitored by the NPP-1000, which includes hardware necessary to read the high-power levels achieved during a pulse. In proposed amended TS 3.2.2, Table 2 specifies the required effective mode protection during pulse. The Percent Power, High Flux Channels from both the NP-1000 and NPP-1000 channels are active during steady-state mode. The neutron flux levels are measured from subcritical source multiplication range through maximum power range. Table 7-4 of the proposed SAR identifies a network virtual terminal (NVT) high (pulsing-only) scram of 50 megawatt-second (MW-s), time integrated power scram setting; however, it should be noted that this scram is not one of the required "Reactor Safety System Scrams" (described above); therefore, it is not relied upon to protect the SL. The licensee stated in the proposed SAR (Ref. 4) that the NVT high scram circuit was always in the scram loop with no associated scram. The setting of 50 MW-s, as the highest indication (labeled on the panel as "MW/SEC"), is provided in Item 4 (Ref. 16). As shown in Table 2, the scrams associated with the pulse mode have a maximum pulse time of 15 seconds and the fuel temperature trip is set at less than or equal to 600°C.

The reactor control system (RCS) monitors and controls operation of the reactor. Power is controlled by four stainless steel-clad borated graphite control rods; three are suspended from electromagnets. The fourth rod (transient) is pneumatically held in place. Using the control console, the operator can also manually withdraw or insert the control rods. During pulse operations, the control system will withdraw the transient rod to rapidly insert reactivity into the reactor core to prompt critical excursion by making a step insertion of reactivity above critical. In pulse mode, the reactor power is measured by the NPP-1000 and the fuel temperature is measured by the NFT-1000.

Independent of the operating mode, the licensee has established the fuel temperature SL at 1,000°C with an LSSS of 600°C. The fuel temperature is measured by three thermocouples in

the reactor and three independent NFT-1000 channels. The I&C systems include fuel temperature and power level scrams to protect and shut down the reactor before the SL can be exceeded. Operators can separately use the manual scram push button to shut down the reactor.

The RPS will shut down the reactor when sensors detect abnormal parameters or when manual actuation devices are activated. The signals that generate a reactor scram are connected to relay contacts in the scram loop. The scram loop consists of normally open relay switches wired in series to provide power to both the control rod magnets and the solenoid for the air supply of the transient rod. During operation, the relay contacts are held closed by power applied to the scram loop. When a scram occurs, the power to the relays in the scram loop is removed and the contacts open. This removes power to the electromagnets of the control rods and to the transient rod air solenoid valve. Consequently, the control rods will fall into the core by gravity. All scram conditions are automatically indicated on the console displays.

Following shutdown, the power exponentially decays and approaches shutdown levels, in which neutron flux level falls to the point where only neutrons from the startup source are observed, and the fuel temperature returns to equilibrium with the bulk coolant. The maximum pulse power is determined by the amount of reactivity inserted by the transient rod. AFRRI TS 3.1.2 defines the pulse mode operation and limits the maximum reactivity in pulse mode.

Section 7.1.1 of the proposed revised SAR, Rev. 1 (Ref. 4) identifies the environmental conditions under which I&C system should operate during normal, abnormal, and accident scenarios. These conditions are identified in Table 1 below.

Table 1 – Environmental conditions for AFRRI

Variable	Operating Range
Temperature	10°C to 40°C
Relative humidity	10% to 90% non-condensing
Pressure	Atmospheric

The AFRRI reactor uses an operating voltage of 120 volts alternating current (VAC) \pm 10%, and 50/60 hertz (Hz). The CSC includes an uninterrupted power supply (UPS), which is connected to the offsite AC power. The LAR Supplement, Rev. 1 (Ref. 4), Section 3 and the proposed TSs (Ref. 18) describes the distribution of AC power from the UPS to the DAC and then to components housed within the DAC. As discussed in Section 3.5.2 of this SE, which is the technical evaluation of the design criteria, if external power is lost, the UPS will initiate a scram and provide power to the control console for approximately 15 minutes to allow the operator to appropriately shutdown the console. The UPS is not a safety-related system and it is not required to power any safety systems. In its April 4, 2022, letter (Ref. 18), the licensee requested to add a new scram channel, AC Power Loss, to TS 3.2.2., Table 2, which, according to the licensee, would ensure a scram in the event of a loss of AC power to the UPS to the control console. Therefore, the licensee notes that providing power to the control console after an AC power loss is not required, but is a desirable feature.

3.2. Data Acquisition Cabinet

Section 3.3 of the LAR, Rev. 1, Section 1 of the LAR Supplement, Rev. 1, and Section 7.2 of the proposed SAR, Rev. 1 (Ref. 4) describe the DAC. The DAC is in the reactor room. The DAC collects reactor data and transmit it to the RCS and CSC. The DAC houses the reactor instrumentation, which consists of NP-1000, NPP-1000, NLW-1000, NMP-1000, and NFT-1000, which are described and evaluated in Section 3.3 of this SE. The DAC also includes the scram loop, the driver and exciter modules for the standard control rod drives, equipment to process analog and digital Input/Output (I/O) signals, and power supplies. Figure 3 in the LAR provides a block diagram of the DAC. Table 1-1 in the LAR, Rev. 1 describes the proposed new equipment and briefly compares it to the old equipment. Table 3-5 in the LAR, Rev. 1 provides the DAC I/O list.

Section 3.3 of this SE describes and evaluates the reactor instrumentation, Section 3.6.1 of this SE describes and evaluates the scram loop, and Section 3.4.1 of this SE describes and evaluates the control rod mechanisms. The following subsections describe and evaluate the DAC equipment to process I/O signals and its power supplies.

3.2.1. I/O Drawers

The DAC includes analog input and digital input drawers to transmit and receive data from the CSC via an air gap Ethernet switch. The DAC acquires data in real-time from the various sensors associated with the reactor and facility. It also receives commands from the CSC and reissues the commands to raise/lower the control rods or scram the reactor.

3.2.2. DAC Power Supplies

The DAC is powered from the UPS located in the CSC. Figure 4 in the LAR Supplement, Rev. 1 (Ref. 4) shows the power distribution for the DAC. This figure shows how power is distributed to power strips. All DAC devices that require AC input power are plugged into these power strips. The power supplies are of the switching type and provide input-to-output isolation with internal overvoltage and overcurrent protection.

3.2.3. Rod Control Drawer

This drawer includes the voltage to frequency (V/F) exciter module and three stepper motor drive modules.

3.2.4. Relay Drawer

This drawer includes the relays associated with the scram loop and magnet power.

3.2.5. Nuclear Instrument Drawers

The DAC includes a linear power drawer, which houses the NMP-1000 and NFT-1000, and a log power drawer, which houses the NP-1000, NPP-1000, and NLW-1000.

3.2.6. Technical Evaluation of the DAC

Since the DAC is a cabinet that houses equipment, the applicable acceptance criteria derived from Chapter 7 of NUREG-1537, Part 2 are:

- A failure or malfunction of equipment, connections, or power supply in the DAC should not prevent the RPS from performing its intended function or prevent safe reactor shutdown.
- The DAC should provide reliable protection to the housed equipment during the normal range of environmental conditions and anticipated events.

In case of a connection/communication failure or malfunction in the I/O boards, the CSC will generate a "Software" scram, opening the relays and shutting down the reactor. The relay contacts in the scram loop require power to remain closed. In case of power loss, the magnets for the control rods and the solenoid for the air supply of the transient rod will be de-energized, dropping the control rods into the core. In addition, in the case of a loss of power to the UPS or UPS failure, the CSC will generate an AC power loss scram, as described in Section 7.2 of the SAR, Rev. 1 (Ref. 4).

The DAC includes most of the electronic components for the I&C system, which generate heat. In Section 1 of the LAR Supplement, Rev. 1 (Ref. 4), the licensee explained that the DAC depends on the reactor room environmental conditions and the venting in the cabinet to limit the expected cabinet heat rise to within the design tolerances of the equipment. The front and rear of the cabinet are perforated to allow for air circulation. Further, air in the control room is continuously circulated, and this is expected to cause flow through the DAC cabinet. In Section 1 of the LAR Supplement, Rev. 1, the licensee also noted that the NIs were tested to withstand temperatures up to 50°C.

Based on the information reviewed, the NRC staff finds that a failure or damage to the cabinets or wires will cause power interruption to the control rod circuitry, which will scram the reactor. Additionally, the operator can initiate a shutdown using manual actuation devices (e.g., manual scram push button on the control panel). Therefore, the NRC staff concludes that the system has been designed to trip the reactor through diverse and independent means, meeting the applicable acceptance criteria derived from NUREG-1537, Part 2.

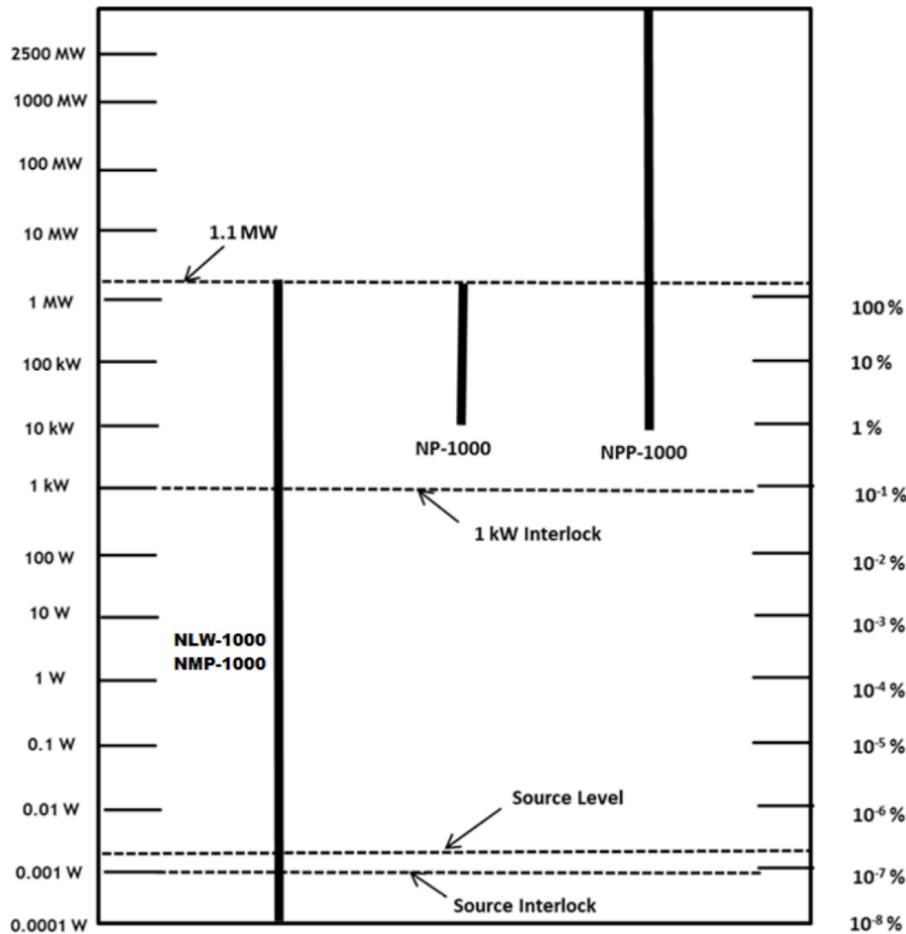
3.3. Reactor Instrumentation

The AFRRl reactor instrumentation includes four independent power measuring modules and one temperature module. These modules provide inputs to the CSC and are evaluated in Section 3.4 of this SE. The modules are used for monitoring and controlling the reactor during startup, normal operation, shutdown, and abnormal conditions. The CSC provides the reactor operator with information and controls to keep the reactor within its operational safety envelope, prevent the reactor from operating if required support systems are not in the proper operating configuration, and initiate automatic protective action if any setpoint is exceeded for reactor period, reactor power, primary coolant flow rate, pool water level, or coolant temperature.

The reactor instrumentation consists of five modules (NP-1000, NPP-1000, NLW-1000, NMP-1000, and NFT-1000) that are housed in the DAC. The DAC is evaluated in Section 3.2 of this SE. The four independent power measuring channels provide a continuous indication of power from the subcritical neutron source multiplication range to the maximum steady-state licensed power level and they provide input to initiate a scram if applicable. Peak power

resulting from the maximum allowed pulse reactivity insertion is monitored by the NPP-1000 module, which is capable of reading the high-power levels achieved during a pulse, up to 6,500 MWt. The temperature module provides three channels to measure fuel temperature, to provide fuel temperature indication, and to provide input to initiate a scram. The location of reactor instrument sensors is shown in LAR, Rev. 1, Figure 3-14 (Ref. 4) and SAR, Rev. 1, Figure 7-6 (Ref. 4).

Proposed SAR, Rev. 1, Section 7.2.2.1, Figure 7-4 (Ref. 4) indicates the power ranges of the channels and the overlap between differing operational modes, which provides sufficient redundancy to offset any potential single failure points. This figure is reproduced below as Figure 2.



- NMP-1000 Compensated Ion Chamber
- NLW-1000 Fission Chamber
- NP-1000 Fission Chamber
- NPP-1000 Fission Chamber (Steady-state Mode)
- Uncompensated Ion Chamber (Pulse Mode)

Figure 2 – AFRR Power Instrument Ranges

3.3.1. NP-1000 Linear Power Channel

Section 1.1 of LAR Supplement, Rev. 1 (Ref. 4) and Section 7.2.2.1.3 of the proposed SAR, Rev. 1 (Ref. 4) describe the NP-1000 linear power channel. The design functions of the NP-1000 provide percent linear reactor power indication (0 to 120%), automatic scram on overpower conditions, analog outputs to the bargraphs and recorders for steady-state operation, and digital outputs to the reactor control console for steady-state operation. The module processes current from a fission chamber. LAR Supplement, Rev. 1 (Ref. 4), Figure 1 reflects that the NP-1000 channel uses the existing fission chamber and a new digital NP-1000 module.

The NP-1000 percent reactor power monitoring instrument is a linear current-to-voltage signal conditioning device that includes a high-voltage power supply, adjustable bistable trip circuits for local and remote alarms, and isolated current or voltage outputs for display by other devices. The NP-1000 unit provides linear power output when the reactor is at power, approximately 1% through 120% power. This channel is designated as Safety Power Channel #1. LAR Supplement, Rev. 1 (Ref. 4), Figure 7, the simplified block diagram for the NP-1000 module, reflects that the input from the detector to the actuation of bistable trips, bargraph, and recorder is retained to the analog portion of the module. The digital conversion of the analog input is used in the control console. The discussion of the trip circuit, as shown in Figure 5 in LAR Supplement 2, Rev. 1, describes how the analog and digital signals are isolated using blocking diodes.

The NP-1000 module has two modes of operation, either local or remote. In local mode, the module accepts commands via the front panel screen. In remote mode, the module accepts commands via the Ethernet port or via the analog remote interface connector on the rear of the panel. The module allows for testing to ensure proper performance. The NP-1000 module consists of seven subassemblies or boards: motherboard, trip/alarm, isolation amplifier, digital interface, display module, front panel, and high voltage (HV) power supply.

Motherboard:

The motherboard serves as the backplane for all other boards. All connections between boards and peripheral devices, such as the front panel display, and remote connectors are made via the motherboard. Incoming signals at the rear of the module are protected by opto-isolators. Outgoing signals are isolated via relays, optical-isolators, or other methods. The motherboard also generates self-test currents from 1 micro-amp to 1 milli-amp representing up to 120% reactor power. The motherboard is calibrated to adjust by 12% every second but can be adjusted via the front panel.

Trip/Alarm:

The trip/alarm board contains six identical circuits to generate all trip and alarm indications. Each circuit can be configured for a rising or falling trip. A comparator monitors input signal and compares it to a reference voltage, which is adjustable. LAR Supplement 2, Rev. 1, Table 2 lists two trips that are the same as the previous design. The trips are: (1) High Voltage low, configured as a decreasing trip when the HV power is below a setpoint (20% loss of HV); and (2) Overpower, an independently adjustable setpoint set for when reactor power exceeds ≥ 1.1 MWt. These trip outputs are inputs to the scram loop, evaluated in Section 3.6.1 of this SE, and are energized in a fail-safe position until an alarm or loss of power de-energizes the coil.

Isolation amplifier:

The isolation amplifier provides two isolated analog output signals that can be configured for voltage (0 to +10 voltage direct current (Vdc)) or current (4 to 20 milli-Amperes (mA)). The isolation is provided by commercial converters that provide 1,500 voltage root mean square (Vrms) galvanic isolation. The isolated outputs provide the analog input for the bargraphs and recorders.

Digital interface:

Digital interface converts the analog signal to digital for use at the reactor control console. This converter, which is a new feature of the NP-1000 module, decreases the distance that the analog signal needs to travel, thus reducing the noise of the signal prior to conversion. It houses the microprocessor, power supplies, analog to digital (A/D) converters, communications circuitry, and the watchdog timer. The watchdog timer monitors the activity of the microprocessor on the digital interface board. If the watchdog timer receives no signal for 1.6 seconds, it causes an alarm that causes the heartbeat light emitting diode (LED) to stop blinking, causing all trips to set, resulting in a reactor scram.

Display module:

The display on the front of the module is a monochrome liquid crystal display (LCD) display with a white LED backlight. The display includes an integrated touch panel with a complete graphical operation system that executes graphical user interface (GUI) applications.

Front panel display:

The front panel display houses red LED indicators for all trips that are activated by the trip/alarm board.

High voltage power supply:

The internal HV power supply can supply up to +1000 Vdc. An internal sense circuit returns 0 to +1 Vdc for an output of 0 to +1000 Vdc.

Technical Evaluation:

The new NP-1000 is designed and manufactured to meet or exceed the requirements of the previous unit. Based on the information reviewed, the NRC staff finds that the updated version of the NP-1000 module maintains adequate independence from the safety function (analog) and from the digital outputs used for steady-state operation (software) and that there is no means for the operator to bypass the scrams associated with the NP-1000, as stated in the TSs and SAR. Review of the AFRRRI Digital Upgrade process for the NP-1000 module is evaluated in Section 3.10 of this SE. The NP-1000 software or anything that the software controls is designed not to impact the safety function of the module in any way. The software performs no safety function. Details and evaluation on independence are in Section 3.7 of this SE.

3.3.2. NPP-1000 Linear Power Pulsing Channel

Section 1.2 of LAR Supplement, Rev. 1 (Ref. 4) and Section 7.2.2.1.4 of the proposed SAR, Rev. 1 (Ref. 4) describe the NPP-1000 linear power pulsing channel. The design functions of

the NPP-1000 provide percent linear reactor power indication (0 to 120%), automatic scram on overpower conditions, analog outputs to the bargraphs and recorders for steady-state operation, and digital outputs to the reactor control console for steady-state operation. Additionally, the NPP-1000 linear power pulsing module measures neutron flux for pulsing operations. The module processes current from a fission chamber for steady-state operations and processes an uncompensated ion chamber or Cerenkov (photon sensing) detector for pulse mode. LAR Supplement, Rev. 1 (Ref. 4), Figure 1 reflects that the NPP-1000 channel uses the existing detectors and a new digital NPP-1000 module.

The NPP-1000 percent reactor power monitoring instrument is a linear current-to-voltage signal conditioning device that includes a high-voltage power supply, adjustable bistable trip circuits for local and remote alarms, and isolated current or voltage outputs for display by other devices. The NPP-1000 also measures reactor power during the pulsing mode of operation. Because reactor power may reach levels several thousand times greater than the maximum steady-state power levels during a pulse, the NPP-1000 has special hardware to measure this condition accurately.

The NPP-1000 provides linear power measurement from approximately 1% power through the pulsing range up to 6,500 MWt and is designated as Safety Power Channel #2. The detection mechanism for the NPP-1000 is chosen based on the mode of operation.

The NPP-1000 has two modes of operation, local or remote. In local mode, the module accepts commands via the front panel screen. In remote mode, the module accepts commands via the Ethernet port or the analog remote interface connector on the rear of the panel. The module allows for testing to ensure proper performance. The NPP-1000 module consists of seven subassemblies or boards: motherboard, trip/alarm, isolation amplifier, digital interface, display module, front panel, and HV power supply, which are similar to the subassemblies evaluated for the NP-1000 evaluated in Section 3.3.1 of this SE, except as noted below.

Motherboard:

The motherboard includes pulse circuitry that produces a current pulse approximately 30 milliseconds to 50 milliseconds wide, with an amplitude of about 1 mA to simulate pulse operation. The detector used during pulse mode (uncompensated ion chamber or Cerenkov detector) is positioned to give a 1 mA detector current for peak pulsed power. The NVT circuit integrates the area under the power curve of the reactor pulse and returns a value that is proportional to the total energy of the pulse. The time to peak and peak detect circuits are used to time low to peak power of a pulse and the hold time of peak pulse.

Trip/Alarm board:

The trip/alarm board contains six identical circuits to generate all trip and alarm indications. Each circuit can be configured for a rising or falling trip. A comparator monitors input signal and compares to a reference voltage, which is adjustable. LAR Supplement 2, Rev. 1, Table 3 lists three trips, which are the same as the previous design. The trips are: (1) High Voltage low trip, configured as a decreasing trip when the HV power is below a setpoint (20% loss of HV); and (2) Overpower, an independently adjustable setpoint set for when reactor power exceeds ≥ 1.1 MWt; and (3) NVT high (pulsing only) set at 50 MW·s. These trip outputs are inputs to the scram loop, evaluated in Section 3.6.1 of this SE, and are energized in a fail-safe position until an alarm or loss of power de-energizes the coil.

Technical Evaluation:

The new NPP-1000 is designed and manufactured to meet or exceed the requirements of the previous unit. Based on the information reviewed, the NRC staff finds that the updated version of the NPP-1000 module maintains adequate independence from the safety function (analog) and from the digital outputs used for steady-state operation (software) and that there is no means for the operator to bypass the scrams associated with the NPP-1000, as stated in the TSs and SAR. Additionally, the pulse data capture is integrated into the instrument and is approximately 10 times faster than the previous system. Review of the AFRRRI Digital Upgrade process for the NPP-1000 module is evaluated in Section 3.10 of this SE. The NPP-1000 software or anything that the software controls is designed not to impact the safety function of the module in any way. The software performs no safety function. Details and evaluation on independence are in Section 3.7 of this SE.

3.3.3. NLW-1000 Log Power Channel

Section 1.3 of LAR Supplement, Rev. 1 (Ref. 4) and Section 7.2.2.1.1 of the proposed SAR, Rev. 1 (Ref. 4) describe the NLW-1000 log power monitor channel. The NLW-1000 is a wide-range logarithmic power monitoring module. It operates with a fission chamber and a PA-1000 preamplifier that decouples and amplifies pulses that originate at the fission chamber. The module combines count rate and current measuring techniques to provide power measurement from the subcritical source multiplication range through full licensed power of 1.1 MWt. In the lower 7 decades, the NLW-1000 counts pulses coming from the PA-1000. In the upper 3 decades, the current flowing in the fission chamber is monitored. The transition from pulse to current mode happens automatically. The combination of the pulse count and the current signal provides a logarithmic indication of the reactor power. The logarithmic reactor power signal is monitored by a period circuit which generates an output proportional to the rate of change in reactor power at any given instant. This signal is called period and it is a measure of the time (in seconds) that it takes for the reactor power to change by a factor of e (2.718). The period indication is from -30 seconds to +3 seconds. The module provides reactor power, reactor period, and isolated analog and digital outputs for use at a console.

The NLW-1000 has two modes of operation, local or remote. In local mode, the module accepts commands via the front panel screen. In remote mode, the module accepts commands via the Ethernet port or the analog remote interface connector on the rear of the panel. The module allows for testing to ensure proper performance. The NLW-1000 module consists of nine subassemblies or boards: motherboard; log count rate board, log current board, analog amplifier; trip/alarm board; isolation amplifier; digital interface; display module; front panel; HV power supply; and the PA-1000 preamplifier. The NRC staff evaluated the NLW-1000 subassemblies or boards for the NLW-1000 module and descriptions and evaluations of the subassemblies or boards are only different from the subassemblies evaluated in Section 3.3.1 of this SE for the NP-1000 in the following ways:

Motherboard:

The NLW-1000 operates in either count rate or current mode, both generated and analog output which then generates a log power signal. Another circuit provides a linear ramp corresponding for a period of 3 seconds for calibration purposes.

Log count rate board:

The log count board produces an output voltage that increases by +1 Vdc per decade increase in count rate. There are sixteen individual circuits designed to be saturated at increasing pulse rates.

Log current board:

The log current board converts feedback voltage into a logarithmic voltage proportional to the current drawn from the HV power supply.

Trip/Alarm board:

The NLW-1000 provides trip outputs for use by the Reactor I&C system for interlock functions: (1) HV Low Interlock (20% loss of HV) used for Control Rod Withdrawal Inhibit; (2) Period Interlock (< 3 seconds) used for Control Rod Withdrawal Inhibit; and (3) Pulse Interlock (> 1 kilowatt (kW) Pulse Interlock) used for Pulse Mode Interlock. These inhibits and interlocks are evaluated in Section 3.4 of this SE.

PA-1000 preamplifier:

The PA-1000 preamplifier decouples and amplifies pulses that originate at the fission chamber.

Technical Evaluation:

The NLW-1000 is one of two new channels to replace the NM-1000. The NLW-1000 is designed and manufactured to meet or exceed the requirements of the previous NM-1000 module. The NLW-1000 provides, independently, both an analog signal and a digital signal to the control console for display (software). The NRC staff finds that the NLW-1000 will continue to perform the design function required by this channel in a safe and reliable manner without imposing any undue risk to the health and safety of the public. Review of the AFRRI Digital Upgrade process for the NLW-1000 module is evaluated in Section 3.10 of this SE. The NLW-1000 software or anything that the software controls is designed not to impact the safety function of the module in any way. The software performs no safety function. Details and evaluation on independence are in Section 3.7 of this SE.

3.3.4. NMP-1000 Multi-Range Linear Channel

Section 1.4 of LAR Supplement, Rev. 1 (Ref. 4) and Section 7.2.2.1.2 of the proposed SAR, Rev. 1 (Ref. 4) describe the NMP-1000 multi-range linear channel. The design functions of the NMP-1000 provide a multi-range percent linear reactor power indication (0 to 120%), provide bistable trips for scrams/interlocks, analog outputs to the recorders for steady-state operation, and digital outputs to the reactor control console for steady-state operation. LAR Supplement, Rev. 1 (Ref. 4), Figure 1 reflects that the NMP-1000 channel uses a new compensated ion chamber and a new digital NMP-1000 module. The NMP-1000 is a microprocessor wide-range linear power module that provides percent reactor power indication and bistable trip circuits. The NMP-1000 module processes current of 1×10^{-11} to 1×10^{-3} A from a compensated ion chamber. The input current is converted into 0 to 10 V in nine one-decade ranges giving power indication from startup through 120% power on a linear scale. The NMP-1000 is an auto-ranging device and will scale itself based on the power level. The operator may also manually select the range locally or from the control console. When the NMP-1000 is in

auto-ranging mode, the overpower scram only occurs on the highest range (i.e., 100% full power or when the range is selected by the operator, and a scram occurs at 110% of that specific range). Both the HV low and the overpower scram trip outputs are wired into the scram loop, however, as shown on Figure 23 of LAR Supplement, Rev. 1 and Figure 7-19 of the SAR, Rev. 1 (Ref. 4), the NMP-1000 scram loop circuit is bypassed.

In the figure in Ref. 21, the simplified block diagram for the NMP-1000 module reflects that the input from the detector to the actuation of bistable trips and recorder is retained to the analog portion of module. The digital conversion of the analog input is used in the control console. The discussion of the trip circuit and as shown in Figure 5 in LAR Supplement, Rev. 1 describes how the analog and digital signals are isolated using blocking diodes.

The NMP-1000 has two modes of operation, local or remote. In local mode, the module accepts commands via the front panel screen. In remote mode, the module accepts commands via the Ethernet port or the analog remote interface connector on the rear of the panel. The module allows for testing to ensure proper performance. The NMP-1000 module consists of nine subassemblies or boards: motherboard, analog amplifier, trip/alarm, isolation amplifier, digital interface, display module, front panel, HV power supply, and compensation power supply, which are like the subassemblies evaluated for the NP-1000 evaluated in Section 3.3.1 of this SE, except as noted below.

Analog amplifier:

The amplifier takes the incoming signal from the detector and converts it into a linear analog voltage in nine one-decade ranges. Each decade of current returns a 0 to +10 Vdc signal. The 1×10^{-11} range is the default and is always active. There are self-tests and calibration available.

Trip/Alarm board:

The trip/alarm board contains six identical circuits to generate all trip and alarm indications. Each circuit can be configured for a rising or falling trip. A comparator monitors input signal and compares to a reference voltage, which is adjustable. LAR Supplement 2, Rev. 1, Table 6 provides a list of outputs for the NMP-1000. The outputs are: (1) High Voltage Low Warning, configured as a decreasing trip when the HV power is below a setpoint (20% loss of HV); and (2) Low Source Count Rate ($< 1 \times 10^{-5}$ watts, replacing the old setting of < 0.5 cps), which provides Control Rod Withdrawal Inhibit interlock evaluated in Section 3.4.4 of this SE. As described in Item 7 (Ref. 16), the NMP-1000 displays power in watts and not in counts per second. The function of the interlock is to only permit rod withdrawal when there are sufficient neutrons to provide sufficient instrument response when bringing the reactor critical.

Technical Evaluation:

The NMP-1000 with the new compensated ion chamber is one of two new channels to replace the NM-1000. The NMP-1000 is designed and manufactured to meet or exceed the requirements of the previous NM-1000 module. The NMP-1000 provides, independently, both an analog signal and a digital signal to the control console for display (software). The NRC staff finds that the NMP-1000 will continue to perform the design function required by this channel in a safe and reliable manner without imposing any undue risk to the health and safety of the public. Review of the AFRRI Digital Upgrade process for the NMP-1000 module is evaluated in Section 3.10 of this SE. The NMP-1000 software or anything that the software controls is

designed not to impact the safety function of the module in any way. The software performs no safety function. Details and evaluation on independence are in Section 3.7 of this SE.

3.3.5. NFT-1000 Fuel Temperature Channels

Section 1.5 of LAR Supplement, Rev. 1 (Ref. 4) and Section 7.2.2.2 of the proposed SAR, Rev. 1 (Ref. 4) describe the NFT-1000 fuel temperature channels. The NFT-1000 is a nuclear fuel temperature module that provides fuel temperature indication, automatic scram(s) on high fuel temperature conditions, analog outputs to the bargraphs and recorders for steady-state operation, and digital outputs for the reactor control console for steady-state operation. The module has three independent channels to process inputs from Type K thermocouples. Temperature transducers convert the millivolt inputs from the thermocouples to usable voltage levels that drive bistable trips for local and remote alarms and that drive isolated current or voltage outputs for display by other devices. The NFT-1000 is calibrated to measure temperature from 0 to 1,000°C.

The NFT-1000 nuclear fuel temperature monitoring module has a capability to measure and capture pulse data, which is temperature values recorded and stored frequently, for a short period during and after a reactor pulse.

LAR Supplement, Rev. 1 (Ref. 4), Figure 20, the simplified block diagram for the NFT-1000 module, reflects that the input from the detector to the actuation of bistable trips, bargraph, and recorder is retained with the analog portion of module. The digital conversion of the analog input is used in the control console. The discussion of the trip circuit and as shown in Figure 5 in LAR Supplement 2, Rev. 1, describes how the analog and digital signals are isolated using blocking diodes.

The NFT-1000 has two modes of operation, local or remote. In local mode, the module accepts commands via the front panel screen. In remote mode, the module accepts commands via the Ethernet port or the analog remote interface connector on the rear of the panel. The module allows for testing to ensure proper performance. The NFT-1000 module consists of six subassemblies or boards: motherboard, trip/alarm, isolation amplifier, digital interface, display module, and front panel, which are similar to the subassemblies evaluated for the NP-1000 evaluated in Section 3.3.1 of this SE, except as noted below.

Trip/Alarm board:

The trip/alarm board contains six identical circuits to generate all trip and alarm indications (two per channel). Each circuit can be configured for a rising or falling trip. A comparator monitors input signal and compares to a reference voltage, which is adjustable. LAR Supplement 2, Rev. 1, Table 7 provides a list of trips for the NFT-1000. The trips are: (1) High Fuel Temp Channel 1 (≤ 600 °C); (2) High Fuel Temp Channel 2 (≤ 600 °C); and (3) High Fuel Temp Channel 3 (≤ 600 °C). The NFT-1000 module provides two bistable trip outputs for each of the three thermocouple channels (1, 2, 3). The TSs require only two fuel temperature measuring channels and associated scrams to be operational. The third channel provides additional redundancy. All trip outputs are inputs to the scram loop, evaluated in Section 3.6.1 of this SE, and are energized in a fail-safe position until an alarm or loss of power de-energizes the coil.

Technical Evaluation:

The new NFT-1000 module is designed and manufactured to meet or exceed the requirements of the previous unit. Based on the information reviewed, the NRC staff finds that the updated version of the NFT-1000 module maintains adequate independence from the safety function (analog) and from the digital outputs used for steady-state operation (software) and that there is no means for the operator to bypass the scrams associated with the NFT-1000, as stated in the TSs and SAR. Review of the AFRRRI Digital Upgrade process for the NFT-1000 module is evaluated in Section 3.10 of this SE. The NFT-1000 software or anything that the software controls is designed not to impact the safety function of the module in anyway. The software performs no safety function. Details and evaluation on independence are in Section 3.7 of this SE.

3.3.6. Technical Evaluation of the Design Bases for the Reactor Instrumentation

The proposed SAR, Rev. 1 provided in LAR Supplement 2 (Ref. 4), Sections 7.2.2.1 and 7.2.2.2 describe the design bases for the reactor instrumentation. The NRC staff finds based on these LAR sections and as described above that the design bases for the reactor instrumentation (NP-1000, NPP-1000, NLW-1000, NMP-1000, and NFT-1000) are adequately described in the SAR.

3.3.7. Technical Evaluation of the Design Criteria

This section of the SE documents the NRC staff's review and evaluation of the proposed reactor instrumentation design to perform its safety functions based on the appropriate design criteria to satisfy the 10 CFR 50.34(a)(3) and 10 CFR 50.34(b) requirements. The staff's evaluation of the design of the proposed reactor instruments is based on acceptance criteria in Sections 7.2, 7.3, and 7.4 of NUREG-1537, Part 2 (Ref. 9).

The licensee identified that the design criteria for the reactor instruments are in Sections 1.1, 1.2, 1.3, 1.4, and 1.5 of LAR Supplement, Rev. 1 (Ref. 4) and Section 7.2 of the proposed SAR, Rev. 1 provided in LAR Supplement 2 (Ref. 4).

The applicable acceptance criteria from NUREG-1537, Part 2, Section 7.4, "Reactor Protection System," are (bulleted items):

- "The design bases for the protection function should be provided."

The proposed SAR, Rev. 1 provided in LAR Supplement 2 (Ref. 4), Sections 7.2.2.1 and 7.2.2.2, describes the design bases for the reactor instrumentation. The NRC staff reviewed these sections and finds that the design bases for the protective functions (NP-1000, NPP-1000, and NFT-1000) are adequately described in the SAR.

- "Detector channels and control elements should be redundant to ensure that a single random failure or malfunction in the RCS or RPS could not prevent the RPS from performing its intended function, or prevent safe reactor shutdown."

Proposed TS 3.2.2, Table 2 shows no changes to the minimum reactor safety systems required for the protective functions. Therefore, the NRC staff relied on the previous staff evaluation, which concluded that the minimum reactor safety systems required for the protective functions are adequate.

- “The logic, schematic, and circuit diagrams should be included and should show independence of detector channels and trip circuits.”

LAR Supplement, Rev. 1 (Ref. 4) provides Table 1 and Figures 8, 11, and 21, which demonstrate that adequate independence is maintained from the safety function (analog) and from the digital outputs used for steady-state operation. The discussion of the trip circuit as shown in Figure 5 in LAR Supplement 2, Rev. 1, describes how the analog and digital signals are isolated using blocking diodes. Additionally, the LAR states that the reactor core is monitored by at least five independent channels that monitor the power level or fuel temperature of the core during steady-state operation and at least three independent channels that monitor the power level or fuel temperature of the core during pulse operations. Therefore, the NRC staff finds that sufficient logic, schematic, and circuit diagrams were included to demonstrate independence of detector channels and trip circuits.

- “The reactor should have operable protection capability in all operating modes and conditions, as analyzed in the SAR....”

LAR Supplement, Rev. 1 (Ref. 4) states that the reactor core is monitored by at least five independent channels that monitor the power level or fuel temperature of the core during steady-state operation and at least three independent channels that monitor the power level or fuel temperature of the core during pulse operations. Therefore, the NRC staff finds that there is adequate protection in all operating modes and conditions, as analyzed in the SAR.

- “The range of operation of sensor (detector) channels should be sufficient to cover the expected range of variation of the monitored variable during normal and transient (pulsing or square wave) reactor operation.”

Proposed SAR, Rev. 1 (Ref. 4), Section 7.2.2.1, Figure 7-4 indicates the power ranges of the channels and the overlap between differing operational modes as depicted above in Figure 2 in this SE. The NRC staff reviewed the information provided and finds that the NP-1000, NPP-1000, NLW-1000, and NMP-1000 ranges are sufficient to cover the AFRR1 reactor from 0.0001 watts to either, in the steady-state mode, up to 1.1 MWt or, in the pulse mode, in pulses of up to 2,500 MWt occurring in about 0.1 second. Additionally, the staff finds that the NFT-1000 temperature range is sufficient to display the design basis limit for fission product barrier protection (i.e., fuel cladding) ultimate fuel temperature limit of 1,000°C.

- “The sensitivity of each sensor channel should be commensurate with the precision and accuracy to which knowledge of the variable measured is required for the protective function.”

Figure 1 of LAR Supplement, Rev. 1 (Ref. 4) shows no changes to the sensors that provide input for the protective functions. Therefore, the NRC staff relied on the previous staff evaluation, which concluded that the precision and accuracy of the variables measured required for the protective function are adequate.

- “Information about the RPS detector or sensor devices should be sufficient to verify that individual safety limits are protected by independent channels, and that LSSS and LCO settings can be established through analyses and verified experimentally.”

Refer to Section 3.6.3(h) of this SE for the evaluation of setpoints.

Based on the information provided and reviewed, the NRC staff evaluated the reactor instrumentation design in accordance with the applicable acceptance criteria in Section 7.4 of NUREG-1537, Part 2. On the basis of the information presented above, the NRC staff concludes that the reactor instrumentation is consistent with the applicable acceptance criteria from NUREG-1537, Part 2.

3.4. Reactor Control System

Section 7.3 of the proposed SAR, Rev. 1, and Sections 1.7 and 2 of the LAR Supplement, Rev. 1 (Ref. 4) describe the reactor control system. The reactor operator uses the reactor control system to perform start up, operation, and shutdown of the TRIGA reactor, as well as control operation in pulse or Square Wave mode. In addition, the RCS maintains the system within licensed limits during normal operation.

The reactor control system includes control rod drives, transient control rod, automatic control, and reactor interlocks. These components are described below. In addition, the RCS includes the control console and display instruments, which are described in Section 3.7 of this SE and consists of the console computer system (CCS) and the User Interface Terminal (UIT). The CCS controls the reactor and monitors all input and output channels. The UIT displays reactor activities and variables monitored. The UIT also captures all events and records them to a file on the UIT computer for later playback.

To operate the reactor, the operator uses the instrument power switch in the Mode Control Panel to turn on the UPS and consequently the CCS. In addition, the Rod Control Panel includes a Magnet Power key switch that must be in the "On" position to power the magnet and the transient rod air circuit, and control movement of the rod controls. Section 3.4 of this SE describes the Magnet Power key switch.

The Reactor Mode Control Panel includes pushbuttons and switches to operate and monitor the reactor. All pushbuttons and switches in the proposed panels, with the exception of the emergency stop pushbutton, provide a digital input to the CSC. The old panel allowed the operator to select the operation mode, but the licensee proposed moving these functions to the CSC to be performed by the software. This is discussed in Section 3.4.3 of this SE.

The status indicators in the Reactor Mode Control Panel are for Core Position, Door Position, Indicators, Pulse Detector Selection, Lamp Test, Emergency Stop, Instrument Power ON, and Watchdog timers for the CCS and UIT computers. The panel has two rotary test switches to test scrams and interlocks. These rotary switches are used to select tests to be performed. These rotary switches are described in Section 3.6.3 (k) of this SE. The Reactor Mode Control Panel also includes switches to move the reactor core to Region 1 and Region 3, and for operating the lead doors. The panel includes three door position switches: Lead Door Open, Lead Door Stop and Lead Door Close. The licensee stated in (Ref. 4) and in Item 9 (Ref. 16) that the addition of the core dolly override switch does not actually move the core dolly, but only permits the core dolly to be moved and is evaluated in Section 3.5 of this SE. The operator can also use the foot pedal, located under the console, to move the core using the pedal corresponding to each region.

In addition, the panel includes a Pulse Detector button, Lamp Test button, Emergency Stop button, and Instrument Power ON. The Pulse Detector is for selecting the type of detector

(Uncompensated Ion Chamber or Cerenkov) connected to the NPP-1000 instrument during pulse. The Lamp test button tests the light bulbs on the Reactor Mode Control Panel. The emergency stop button will shutdown the reactor without intervention from the CSC. The emergency signal is part of the FIS and upon pressing it, deactivates the reactor permissive (ROX) relay that is an input to the Scram loop. The Emergency Stop is a latching switch; the first push activates it; the second push deactivates it. The Instrument Power ON button is used to activate or deactivate the UPS.

The reactor has three standard control rods (one regulating rod, one shim, and one safety) and a transient rod. The RCS allows individual control rod withdrawal and prevents withdrawal of more than one rod at a time. A function can insert all control rods simultaneously to reduce reactivity. In Auto mode, the operator can move rods using the bank selections: Reg only; Reg and Shim; Reg, Shim and Safety. The rod withdrawal interlock inhibits outward rod motion under certain conditions. The transient rod was not modified. The licensee proposed modification of the rod controls and drives for the three standard control rods. These rod controls are described in Section 3.4.1 of this SE.

The DAC provides interfaces between several systems and the RCS. The DAC provides input signals to the RCS to determine the current conditions of the reactor and other components. The DAC also transmits output signals generated by the RCS to control equipment and auxiliary. The DAC is described in Section 3.2 of this SE.

The reactor instrumentations provide inputs to the RCS for display by the bargraphs, chart recorder, and UIT computer display interface. The RCS also uses these signals in the logic to scram the reactor, as well as to provide indication of the current core conditions on the display screens and provide feedback on reactor conditions during movement of the control rods, neutron source, and fission chamber. The reactor instrumentations are described in Section 3.3 of this SE.

3.4.1. Rod Control and Rod Drives

Section 7.3.1 of the proposed SAR, Rev. 1 and Section 1.7 of the LAR Supplement Rev. 1 (Ref. 4) describe the control rod drive mechanisms (CRDM). The control rod drives control all data acquisition and display functions to manipulate reactivity in the core at the appropriate time.

There are three standard control rods and a transient rod. The standard rod drives are coupled to an electromagnet to control their movement and the transient rod has an air circuit. In the previous system, two CRDMs are fixed speed, and one is variable speed. In the proposed CRDMs, all three rods are variable speed to allow fine control in automatic mode and the potentiometer in the driver sets the maximum speed possible, which was increased from 0.42 to 0.5 inches/second. Section 1.7.3 of the LAR Supplement Rev. 1 compares the old and new CRDMs.

The control rod drives are connected to the control rods through a connecting rod assembly. The proposed control rod drives are rack and pinion type, which are driven by stepping motors. The pinion gear engages a rack attached to the magnet draw tube. The stepping motors operate on phase-switched direct current (DC) power. The motor shaft advances 500 steps per revolution (0.72° per step) when in full-step mode. In the LAR Supplement Rev. 1, Section 1.7.4.4, AFRR1 noted that the factory settings are near the maximum values and exceed the requirements for this application, which is required because of the limit on maximum reactivity

insertion rate. The drive speed and the differential rod worth determine the reactivity insertion rate.

The exciter module is used to control the stepper motor driver modules. It consists of a motherboard and several voltage to frequency oscillator daughter boards. The operator selects the control voltage in the control console. There are analog control voltages from +10 to -10 Vdc for each rod drive. This signal is converted to pulse trains with frequencies proportional to the amplitudes of the voltages. These pulse trains are then fed into the stepper motor driver modules. Positive voltages will drive the rod up, and negative voltage will lower the rod. The maximum speed is set by a combination of the driver hardware and software configuration, which are only available via password-protected computer access or locked cabinet hardware access.

The licensee proposed a rod control drawer (see description in Section 3.2.3 of this SE) to store the voltage to frequency exciter module, three stepper motor driver modules and limit switches. These items are powered from the DAC AC power.

As the rod drives travel through their range of operation, the potentiometer provides the rod position, which is transmitted by drive communication channels in the DAC and thereby presented to the operator. In addition, the up/down rod control signals, limit switch signals, and magnet power are transmitted to the DAC. The licensee stated in Ref. 4, that the wiring for the rod control system and the rod drive assembly, is installed on the reactor bridge. AFRRI staff explained that all cables from the DAC to the connecting rod assembly were replaced, but wires from the assembly to the control rod drive were not replaced. The NRC staff observed the new wires but noticed that the cables were not labeled, and the connections included cables that were no longer in use. The AFRRI staff noted that there were no requirements to remove the cables and that testing ensured that the correct cables were connected. The logic is handled in the control console, which is described in Section 3.4.3 of this SE.

The control console includes a Rod Control Panel to operate the control rods. Section 3.7.6 of this SE describes the rod control panel.

The CRD includes the following limit switches to indicate position of the rod and magnet. The licensee proposed replacing the limit switches, but they perform the same functions.

- Rod DOWN – for indication of the control rod at the lower limit of travel
- Magnet UP – for indication of the magnet at the upper limit position
- Magnet DOWN – for indication of the magnet at the lower limit position

When the limit switches for the magnet are active, they stop the movement of the control drive. Figure 7-14 in the proposed SAR Rev. 1 (Ref. 4) shows the location of these limit switches. The position of the control rod is inferred by a combination of the Rod DOWN and magnet DOWN/UP limit switches.

3.4.2. Transient Rod Control

The AFRRI TRIGA reactor is designed for pulsing or "square-wave" operation mode. The transient rod rapidly inserts positive reactivity in these modes. The transient rod is operated by a pneumatic/electric drive. A connecting rod couples the transient rod to a piston rod assembly. When the air solenoid valve is energized air pressure is placed on the bottom of the piston, causing the piston to be brought in contact with the shock absorber. The resulting reactivity

insertion is dependent on the position of the cylinder before applying air. Scram of the transient rod is accomplished by deenergizing the air solenoid valve. This vents the air pressure under the piston and results in the control rod dropping. The transient rod can also be used in manual mode like the standard control rods. The licensee did not propose any changes to the existent transient rod control, except for the cables connecting the rod driver to the DAC, as discussed in the audit. Section 7.3.2 of the proposed SAR Rev. 1 (Ref. 4) describes the transient rod.

3.4.3. Modes of Operation

The old Reactor Mode Control panel included pushbuttons and switches necessary to control the reactor. In the LAR, the licensee proposed moving certain functions to the CSC, including the reactor selection mode. Consequently, the proposed Reactor Mode Control panel does not include pushbuttons for selection of the reactor operation mode. Sections 3.2.3 and 3.4.4.1.4 of LAR Supplement Rev. 1 and Section 7.6.4.2.1 and Figure 7-30 of the proposed SAR Rev. 1 (Ref. 4) describes the CSC console, in which the operator can select the reactor mode of operation using the MODE SELECTION pane in the console. The RCS can be operated in the following modes:

- Manual (or steady-state) mode, in which the reactor can operate up to 1.1 MWt. In this mode, the operator uses the UP or DOWN pushbuttons for the transient, shim, safety, or regulating rods in the Rod Control Panel. These signals are transmitted to the CCS, which translate this to voltage for the drive to move the rods in the up or down direction. These pushbuttons shown in Figure 7-17 in the proposed SAR Rev. 1 (Ref. 4).
- Automatic (sometimes known as auto or servo) mode, in which the reactor can operate up to 1.1 MWt. In this mode, the rods are moved based on the evaluation of signal from the NMP-1000 power measurement and the NLW-1000 period measurement in order to maintain the power demand selection. From this mode, the operator can return to manual mode by pressing the (software) Manual button on the status screen in the control console.
- Square Wave mode, which uses the transient rod to increase power up to 1.1 MWt. This mode can only be used when the reactor is operating in steady-state mode. With the power less than 1,000 watts (as determined by the NLW-1000) and the transient rod air supply turned off, the Square Wave mode switch can be depressed. The rod control console includes the FIRE button, which can be pressed to initiate this mode. The Square Wave mode switch is depressed which makes the mode change. This will change the console from steady-state to Square Wave mode. Once the desired level is reached, the console will switch to automatic mode to maintain the power level. If the desired power level is not reached within 30 seconds, the system will switch to Manual Mode and display a message to the operator on the annunciator pane.
- Pulse mode, which is used for a large-step insertion of reactivity results in a short duration reactor power pulse. The reactor power pulse is a function of core physics and typically lasts a few hundred milliseconds. Also, the operator can manually scram the reactor after a few seconds or define a duration for automatic scram using the Set Pulse Time limit. The NLW-1000 controls the 1 kW interlock. If pulse is selected and the operator presses the FIRE button, the system will check that power is less than 1 kW and activate the PULSE INHIBIT in the NLW-1000 to disconnect the logarithmic current amplifier circuit.

In Item 3 (Ref. 16), the licensee explained that the control console included a bypass to inhibit the overpower scram of the old NP-1000 during pulse mode. With the proposed amendment, this software-based function was added to the NLW-1000 and NMP-1000.

Using the MODE SELECTION pane in the console, the operator can also:

- Enter a demand power setting in Watts using the text box and button for this.
- Manually select the NMP-1000 range. The NMP-1000 can operate in manual range or automatic range. When in manual, the software will prevent the NMP-1000 from scaling itself based on the power level. If the power continues to rise and the NMP reaches 110% of its selected scale, it will initiate a scram in the scram loop, however, the NMP-1000 contacts are bypassed in the scram loop, and therefore no scram occurs. When in automatic range, in normal operation, the NMP will change its scale based on the reactor power. The NMP range selection is displayed in the Mode Selection Pane.
- Define a timed actuation to select the length of time before an automatic scram after a reactor pulse. There are buttons to start, stop, and reset this timer. It may be directed to count up or count down.

The operator can scram all control and transient rods at any time in any mode of operation by pressing the SCRAM button on the rod control panel. The operator can also use the AIR push button and MAGNET pushbuttons on the rod control panel to remove air from the transient rod and magnet power for the Shim, Safety and Regulating rods, respectively.

The reactor control system has the following defined states:

- The time delay state, which begins when no emergency stops are active, all facility interlocks are satisfied, and the magnet power key switch is turned to Reset. This initiates a 30-second countdown and given no interrupts, the system proceeds to the operate state.
- The operate state, which allows magnet power to be applied. This requires turning the magnet key switch to Reset and the operator to move control rods to insert reactivity.
- The steady state, which maintains power during operation.
- The scram state, which occurs when a fault is detected during operation. Any fault on the scram loop removes magnet power (and air pressure to the transient rod) releasing the control rods and allowing gravity to fully insert the rods into the core.
- The test state, which occurs when the reactor has been scrammed and the operator is testing various inputs and functions.

The logic for controlling the reactor is part of the proposed CSC. The operator interface includes the necessary controls and interfaces for the operator to manipulate the control rods and monitor operating parameters during various modes of operation. Also, using the control console, the operator can select rods for the bank movement, including Reg only; Reg and

Shim; and Reg, Shim and Safety. The CSC is described and evaluated in Section 3.7.1 of this SE.

3.4.4. Rod Withdrawal Prohibits

Section 7.3.4 of the proposed SAR Rev. 1 (Ref. 4) describes and lists all of the rod withdrawal prohibits (RWP). In Item 1 (Ref. 16), the licensee clarified that they use term rod withdrawal prevent, prohibit, or rod withdrawal inhibit or interlock (RWI) interchangeable in their documents. The RWP function is to prevent inserting positive reactivity into the core until specific conditions are satisfied. The RWP does not prevent lowering the control rods or scrambling the reactor. The logic for the RWP is implemented in the CSC. The RWP includes an interlock to restrict any rod withdrawal if certain signals from the NLW-1000, NMP-1000, and inlet water temperature are present.

LAR Supplement Rev. 1, Section 1.7.6, TS 3.2.2, Table 3 (Ref. 4) identifies the minimum reactor safety system interlocks, which are:

- Pulse initiation at power levels great than 1 kW (only for pulse mode)
- Withdrawal of any control rod except transient (only for pulse mode)
- Any rod withdrawal with count rate below 1×10^{-5} watts as measured by the operational channel (steady state and pulse modes)
- Simultaneous manual withdrawal of two standard rods (steady state mode)
- Any rod withdrawal if high voltage is lost to the operational channel (steady state and pulse modes)
- Withdrawal of any control rod if reactor period is less than 3 seconds
- Application of air if the transient rod drive is not fully down. (This interlock is not required in square wave or pulse modes)

These reactor safety system interlocks are required to be tested daily whenever operations involving these functions are planned.

Section 2.1.4.2.1.4 of the system requirements specification (SYR), "Reactor Display 1," which was reviewed as part of the audit (Ref. 5) identifies the interlocks to be displayed in the control console:

- PI: NMP Low Src, to indicate low source level
- PI: NLW Period, to indicate that period circuit not active in Pulse mode
- TR: NLW 1 kW, which refers to the 1-kW permissive interlock to prevent pulsing when wide-range log power is above 1 kW
- RWP: NLW HV Low, to indicate low high voltage
- RWP: Two Up, to indicate that two up buttons are pressed up simultaneously
- RWP: Demin Temp, to indicate high temperature in the inlet
- RWP: Low Pool, to indicate the level is approximately 2 in below
- TR: Fire invalid, to indicate that the Fire button is disabled
- TR: Two Up, to indicate that two up buttons, not counting TR UP
- "RWP: NP, NPP, NFT, NLW, NMP Loss of Comms," (this interlock was not included in the as-built configuration)

The licensee stated in LAR Supplement Rev. 1(Ref. 4) and in Item 2 (Ref. 16), that the "loss of Comms" does not provide an interlock and therefore is not shown on the INTERLOCKS PANE.

In addition, Item 2 (Ref. 16) also clarified that PI: "NLW Low Src" was incorrect and should be "NMP Low Src." The abbreviation for Low Source is Low Src.

In Item 2 (Ref. 16), the licensee provided a cross reference between the interlocks required and those displayed.

The status of these interlocks will be shown in the INTERLOCKS PANE shown in the Reactor Display 1 tab in the control console. These interlocks include an alarm disable check box. By default, these indications are disabled, so a message won't appear in the annunciator pane. Section 3.7 of this SE describes the control console. Further information was provided in the Site Acceptance Test 1 (SAT1), Section 1.2.7 and tested in SAT1 Section 2.3.4.2, which the NRC staff reviewed during the audit.

In Item 2 (Ref. 16), the licensee explained that this pane does not include all interlocks, and it only shows those that require rod motion up. This reference also describes the operation mode in which the UP buttons are disabled.

3.4.5. Technical Evaluation of the Design Bases of the Reactor Control System

This section of the SE documents the NRC staff's review and evaluation of the design basis of the reactor control system against the design bases acceptance criteria in Section 7.3 of NUREG-1537, Part 2.

As part of the LAR, the licensee submitted a proposed Section 7 of the AFRRRI SAR. Section 7.1.2 of the proposed SAR identifies the design bases for the AFRRRI TRIGA reactor. The NRC staff reviewed and evaluated the RCS design basis to determine the adequacy of the control systems to maintain the required variables within operational limits during facility operation and to verify that the impact of control system failures is appropriately included in the SAR accident analyses. Based on the system description, confirmed in part by the NRC staff observations of the equipment during the audit (Ref. 5), the NRC staff finds that the RCS design meets the design acceptance criteria in the guidance in Section 7.3 of NUREG-1537, Part 2 and that the instrumentation provides continuous indication of the neutron flux over the licensed maximum power range and entire expected range of the monitored process variables, as defined in the AFRRRI TS, and that suitable alarms and/or indications are provided. The NRC staff finds that the detector channels in the RCS directly monitor neutron flux for reactor power level and power rate-of-change, and interlocks are in place to prevent reactor startup without a sufficient neutron count rate in the core or other unsafe conditions.

The proposed nuclear instruments will monitor the neutron flux and reactor power at the same range as the previously approved channels. The nuclear instruments provide information to both the RCS and the RPS portions of the system to allow them to monitor reactor conditions during normal and accident conditions. This information also provides the capability for periodic testing, channel checking and calibration of the I&C system. In addition, the nuclear instruments provide an independent, diverse, and redundant method to initiate a reactor scram. The scram signals generated by the nuclear instruments will interrupt power to their corresponding relay in the scram loop. During the audit (Ref. 5), the NRC staff observed that the nuclear instruments have sufficient range to cover the expected ranges of the monitored variables during normal operation and reactor transients, as stated by the licensee in the LAR.

The radiation protection system is not connected with the RCS. This system is housed in an auxiliary console adjacent to the main console and displays the radiation levels at select

locations throughout the facility. In this manner, the operator can monitor radiation levels and perform safety actions (e.g., scram), if necessary.

In the LAR, the licensee proposed replacing the CDRMs and limit switches to control the position of the reactor. The RCS is connected to the CRDMs to generate the signals necessary to move the core. The limit switches interface with the RCS, via the DAC, to indicate the location of the reactor. In Section 1.7.5 of the LAR Supplement, Rev. 1 (Ref. 4), the licensee provided a safety analysis describing the adequacy of the design to establish conformance to the design criteria and design bases for reactor power, rate of power change, and pulsing information. In the LAR, the licensee stated that a failure of the CRDM won't affect the operation of the RPS. The scram loop includes independent relays associated to the different safety functions performed by the nuclear instruments. In addition, the licensee identified that the bounding accident associated with the CRDMs is the simultaneous withdrawal of all three standard control rods resulting in a ramp insertion of excess reactivity. This accident was analyzed in the SAR submitted as part of the license renewal. In the LAR, the licensee explained that this analysis remains valid since the ramp insertion of excess reactivity scenario is mitigated by the three second period interlock and not the speed of the control rods.

During the review of the reactor control system, the NRC staff examined the logic for the rod withdrawal prohibits. The RWP ensures safe operation of the reactor in accordance with the requirements in TS 3.2.2, but they do not generate a signal to scram the reactor. The rod drives themselves do not provide any safety function. In the event of a scram, the magnets are de-energized (or air pressure released for the transient rod drive) and the control rods are dropped into the core by the force of gravity, while the drives are driven to their bottom limit. To prevent a scenario in which the safety limit could be threatened, or otherwise unsafe conditions created, interlocks are provided to prohibit rod withdrawal. The NRC staff reviewed the factory acceptance testing (FAT) and site acceptance testing (SAT) results during the audit (Ref. 5) and confirmed that the tests demonstrated proper functionality of the RWP.

The RCS will generate several software scrams, a scram signal when communication with any COTS I/O board is interrupted, CCS watchdog timer, and UIT watchdog timer. During the audit (Ref. 5), the NRC staff reviewed these software generated scrams and their signals in the scram loop to gain a better understanding of the detailed bases underlying the information submitted by the licensee in the LAR Supplement Rev. 1 and SAR Rev. 1 (Ref. 4). The software generated scram signal provides a diverse and redundant backup to the other signals in the scram loop. Also, during the audit, the NRC staff reviewed the results from the factory FAT and SAT and confirmed that functionality of these software generated scrams were successfully tested, demonstrating that they would perform their function per the design bases requirements stated in the LAR.

The RCS will also generate an inhibit signal when the reactor is in Pulse mode (Ref. 16). This inhibit-signal bypasses the scram signals from the NLW-1000 and NMP-1000. This signal was part of the previous system, and was added since the AFRRI TS does not require the NP and NPP overpower scrams during pulse mode operation, and only the NPP is required to perform a high-power scram, as described in Section 3.6.2 of this SE.

ANSI/ANS-10.4-1987 provides guidance for the verification and validation (V&V) of scientific and engineering computer programs for the nuclear industry. Section 9 of the standard recommends that the test results for the V&V activities during the installation phase be documented and reported as specified in the V&V Plan and, if the findings necessitate any retesting or revision of the test report, the updated test results should be verified again before

final program acceptance. During the audit (Ref. 5), the NRC staff reviewed the design and testing processes of the I&C system, as described in the LAR, and observed that the licensee and its vendor followed them. In addition, during the audit, the NRC staff reviewed the FAT and SAT to confirm that the system was successfully tested.

During the audit, the NRC staff observed operation of the control system from the control console. The licensee demonstrated movement of the core, opening/closing the lead doors, alarms, warnings, etc. Also, the NRC staff observed the configuration of the screen and displays in the proposed control console. The displays are configured to indicate when any condition that causes a scram, interlocks, or warnings. These design features and the information available to the operator provide the capability for periodic testing, channel checking and calibration of the I&C systems.

To ensure continuous monitoring and control by the RCS, the licensee selected components suitable for the environmental operating conditions in the reactor room and control room. AFRRRI noted that if the I&C system were affected by the environmental operating conditions in these rooms, this will potentially affect communication with the control system, which will then scram the reactor. The heating, ventilation, and air conditioning (HVAC) in AFRRRI is separate equipment and it does not interface with the RPS and RCS. The HVAC system ensures acceptable environmental limits are maintained.

The RPS has been designed to scram the reactor given several conditions, which are described in Section 3.3 of this SE. These scram relays are independent of the RCS and any failure or operation of the RCS is overridden by the scram loop, which results in a scram by removing magnet power and dropping the control rods into the core. Chapter 7 of the proposed SAR is included in the LAR and identifies that the primary design bases for the AFRRRI reactor is the safety limit on fuel temperature, which is independent of any action the RCS can take. Even though the RCS is not credited for maintaining fuel temperature, failure of the RCS would automatically open its associated scram relay in the scram loop. If the RCS scram relay did not operate as intended, the remaining RPS scram relays would independently scram the reactor.

The NRC staff evaluated the RCS design using the design basis acceptance criteria identified in Section 3.1 "Design Criteria," and Section 7.3, "Reactor Control System," of NUREG-1537, Part 2. Based on the information provided by the licensee and reviewed by the NRC staff, the NRC staff finds that the RCS design basis results in a reliable, redundant, and fail-safe system that helps ensure continued operation of the reactor within the safety limit established in the AFRRRI TS.

Based on the NRC staff's review of the information provided in the LAR, as supplemented, and supported by the observations during the audit, the NRC staff concludes:

- RCS design criteria supporting the design bases are specified for the portions of the RCS that are assumed in the SAR to perform an operational or safety function.
- The design bases functions of the RCS and components are designed to permit and support normal reactor operations, and the RCS and its subsystems and components will give all necessary information to the operator or to automatic devices in order to maintain planned control for the full range of normal reactor operations.
- The licensee included RCS design criteria and provided references to relevant up-to-date standards, guides, and codes, which includes information on the design:

- for the complete range of normal reactor operating conditions;
 - to cope with anticipated transients and potential accidents;
 - redundancy to protect against unsafe conditions in case of single failures of reactor protective and safety systems;
 - to facilitate inspection, testing, and maintenance; and
 - quality standards commensurate with the safety function and potential risks of the AFRRRI TRIGA reactor.
- RCS design criteria supporting the design bases are derived from applicable standards, guides, codes, and criteria and provide reasonable assurance that:
- the structures, systems, and components of the RCS will function as designed and required by the analyses in the SAR; and
 - the public will be protected from potential radiological risks resulting from operation of the RCS system and subsystems.

3.4.6. Technical Evaluation of the Design Criteria

This section of the SE documents the NRC staff's review and evaluation of the proposed RCS system design to perform its safety functions based on the appropriate design criteria to satisfy the 10 CFR 50.34(a)(3) and (b) requirements. The NRC staff's evaluation of the design of the proposed RCS I&C systems is based on acceptance criteria in Section 7.3 of NUREG-1537, Part 2, including guidance in industry standards referenced by Section 7.3 of NUREG-1537.

(a) Independence

Section 7.4 of NUREG-1537, Part 2, states that the SAR should address the separation and independence of the RCS and RPS and show independence of detector channels and trip circuits. However, given the acceptable small or insignificant radiological risk to the public or to the environment, NUREG-1537 further states:

If the safety analysis in the SAR shows that safe reactor operation and safe shutdown would not be compromised by combination of the [RCS and RPS], they need not be separate, independent, or isolated from each other.

NUREG-1537, Part 2 also states that hardware and software for computerized systems should meet the guidelines of IEEE 7-4.3.2--1993 (Ref. 11). IEEE 7-4.3.2 states that safety functions be separated from non-safety functions such that the non-safety functions cannot prevent the safety system from performing its intended functions. Appendix E of IEEE 7-4.3.2 further states that “[f]or proper independence of the safety computer from non-safety equipment, both electrical and communication isolation should be ensured.”

In Section 1 of the LAR, the licensee stated that RCS monitors many of the same parameters as the RPS and gives information for automatic and manual control. In the LAR Supplement Rev. 1 (Ref. 4), Section 1.6.5, the license stated that the RPS is completely independent of other systems including the RCS. Independence between the reactor instruments is evaluated in Section 3.3 of this SE.

Data and signals from the reactor instruments and control systems are transmitted to the control console through the DAC, which uses an air gapped ethernet cable connection. These signals are used for indication of reactor power level, fuel temperature, and period on bargraph meters and chart recorders. These devices obtain their signal directly from the analog output of the respective monitoring unit and have no interface with other equipment.

The data from the radiation monitoring system is displayed on the auxiliary console and does not interface with control system console. The auxiliary console also provides indication for pool temperature, pool level, exposure room temperatures, and ventilation dampers, as described in Section 3.7.10 of this SE.

During the audit (Ref. 5) the NRC staff observed the location and configuration of the proposed I&C system and confirm the physical, electrical, and communication independence between the different systems. Thus, any interactions among them would not result in compromising the function of the safety system. The NRC staff confirmed that the nuclear instruments provide input to both the RCS and the RPS, and the signals send to these devices are separated. Although the cabling is located in the same cabinet and routed together, separate cables carry the signals to the RCS and RPS.

Based on the information provided, the NRC staff finds that the reactor control system design includes independent means to protect the reactor if any single component or channel fails. Therefore, the NRC staff finds that the proposed I&C system meet the intent of the design acceptance criteria applicable to research reactors for independence identified in IEEE 7-4.3.2-1993 and the guidance in Section 7.3 of NUREG-1537, Part 2.

(b) Fail-safe on Power Loss

The fail-safe design acceptance criteria of NUREG-1537, Part 2 help to ensure that, on loss of power, the control system and associated equipment are designed to assume a safe state and will enable safe reactor shutdown.

LAR Supplement Rev. 1 (Ref. 4), Section 1.6.5, states that the system is designed to be fail-safe because whether a loss of power or any damage due to fire, explosion, dropped load, or some other cause results in a loss of power to the electromagnets that connect thee control rods and control rod drives, causing the control rods to drop into the core.

Based on the information provided in the LAR, SAR, and its audit observations, the NRC staff finds that the licensee's implementation of fail-safe acceptance criteria for the reactor control system is acceptable. The NRC staff finds the reactor control system design includes redundant methods to help ensure the reactor assumes a safe state on loss of electrical power. Therefore, the NRC staff concludes that the design of the reactor control system meets the fail-safe acceptance criteria in Section 7.3 of NUREG-1537, Part 2 which are that the systems assume a safe state, enable safe reactor shutdown, and not prevent the RPS from performing its designed safety function.

(c) Effects of Control System Operation/Failures.

The proposed RPS is designed to scram the reactor on a number of conditions, which are detailed in Section 3.6 of this SE. These scram relays are independent of the control system and any failure or operation of the control system is overridden by the scram loop opening resulting in a scram, which will remove magnet power and drop the control rods into the core.

Based on the information provided, the NRC staff finds that the design of the I&C system help ensure the reactor assumes a safe state even if the reactor control system were to fail completely. Therefore, the NRC staff concludes that the proposed I&C system meet the fail-safe acceptance criteria in Section 7.3 of NUREG-1537, Part 2, which are that the systems assume a safe state, enable safe reactor shutdown, and not prevent the RPS from performing its designed safety function in the case of control system action or inaction.

(d) Operational Bypass

Other than the operator bypass switches in the exposure rooms, the licensee stated in Section 2.5 of LAR Supplement Rev. 1 (Ref. 4) that there are no means for the reactor operator to manually bypass any interlocks. The system includes bypasses to inhibit operation of certain devices during a pulsing operation (Ref. 16). These bypasses are programmed in the software, and it cannot be modified by the operator.

The purpose of the bypass switches in the ER is to inhibit the horns in the ER to accommodate the needs of experiments that are sensitive to noise.

Based on its review of the information provided above, the NRC staff concludes the design of the bypasses and interlocks meet the design acceptance criteria in Section 7.4 of NUREG-1537, Part 2 and ensure operable protection capability in all operating modes and conditions, as analyzed in the SAR by ensuring there are no means for the operator to manually bypass any interlocks.

(e) Surveillance

The guidance in Section 7.3 of NUREG-1537, Part 2, recommends application of the functional design and analyses to the development of bases of technical specifications, including surveillance tests and intervals. Additionally, ANSI/ANS-15.15-1978 recommends the system design include capability for periodic checks, tests, and calibrations. The standard also recommends that, if online periodic testing is necessary, such testing should not reduce the capability of the system to perform its safety function.

Based on the TSs evaluation in Section 3.11 of this SE, the NRC staff concludes the design of the control system meets the design acceptance criteria in Section 7.3 of NUREG-1537, Part 2. This includes the capability for periodic checks, tests and calibrations to facilitate the performance of the required testing to ensure control system operability without affecting the capability to perform its intended function, and that the control system testing provisions, and the bases for technical specifications including surveillance tests and intervals provide reasonable assurance of the continued reliable operation of the control system.

(f) Quality

The quality for the proposed systems is reviewed under the section on evaluation of digital upgrade process, Section 3.10 of this SE. This section describes the licensee's overall quality assurance program (QAP) for the proposed I&C system.

Based on the evaluation of the information presented in this SE, the NRC staff concludes:

- The licensee has considered the normal operating characteristics of the reactor facility, including thermal steady-state power levels, and the planned reactor utilization for the proposed I&C system. The system design continues to provide the necessary functions of the control system and components to permit and support normal reactor operations, and provides all necessary information to the operator or to automatic devices to maintain planned control for the full range of normal reactor operations.
- The components and devices of the reactor control system are designed to sense all parameters necessary for facility operation with acceptable accuracy and reliability and to transmit the information with high accuracy in a timely fashion. In addition the control devices are designed for compatibility with the analyzed dynamic characteristics of the reactor.
- The proposed design preserves the TS-required interlocks, and provides suitable redundancy and diversity to avoid a total loss of operating information and control, to continue to help limit hazards to personnel, and to help ensure compatibility among operating subsystems and components in the event of single isolated malfunctions of equipment.
- The design of the proposed I&C system is such that any single malfunction in its components would not prevent the RPS from performing necessary functions, nor prevent achieving a safe shutdown condition of the reactor.
- The provisions for channel tests, checks, and calibrations, and the bases for surveillance tests and intervals provide reasonable assurance that the reactor control system will function as designed.
- The design for pulsing or "square-wave" operation, the transient rod and its driver mechanism, interlocks, mode switching, detector channels, other related instruments, and limiting technical specifications are designed for the highest possible reliability to ensure that analyzed fuel safety limits will not be exceeded, and personnel hazards will be controlled.

3.5. Facility Interlock System

Section 2 of the LAR Supplement Rev. 1, Section 7.3.5 of the proposed SAR Rev. 1 (Ref. 4), and Section 2.3.21.4 of the Functional Requirements Specification (FRS) and errata (Ref. 15), describe the proposed facility interlock system (FIS). The purpose of the FIS logic is to prevent accidental radiation exposure of personnel working in the ERs or the preparation area. It also prevents interference (i.e., contact or impact) between the reactor tank lead shield doors and reactor core shroud.

The proposed FIS uses limit switches and pushbuttons to implement the logic that prevents inadvertent operation of the facility when a set of conditions have not been met. Figure 7-18 in the proposed SAR, Rev. 1, depicts the FIS block diagram. The licensee stated in (Ref. 4), that this diagram was derived from the original truth table for the FIS interlock, which shows all possible combinations to test the validity of the logic.

The FIS interfaces with the console, magnet power keyswitch, and DAC via relays to electrically isolate the various systems. The relays are housed in a stand-alone central cabinet, which also includes various peripherals such as motor control centers (MCC), horns, and limit switches. These components are described in the subsections below.

The FRS states that the logic depends on the positions of the reactor core, the reactor tank shield doors, and the plug doors to the ERs. The reactor core positions are classified into three regions: Region 1, Region 2, and Region 3. Using the Reactor Mode Control Panel, the operator could open/close the lead shield doors using the pushbuttons in the panel. In addition, this panel includes a pushbutton to stop movement of the lead door. These switches will illuminate when activated. During the audit (Ref. 5), AFRRRI demonstrated operation of the lead door to enter ER #1 (fast neutron) in the facility floor. Also, during the audit, the NRC staff observed location of the ERs, the plug doors and ER control boxes for ERs #1 and #2.

The FIS will sound a horn in the necessary ERs, ER #1, or ER #2 for 30 seconds when the reactor is about to start operation. For an experiment sensitive to noise, the operator can bypass the horn in the ER using the operator bypass switches in the ER and in accordance with AFRRRI administrative procedures. During the audit, the NRC staff reviewed the AFRRRI Maintenance Procedure, M033 – Facility Interlock Checklist, completed on February 27, 2018, which requires verification of interlocks, horns, horn bypass switches, and status lights for the ER.

In Section 2.4 of the LAR Supplement Rev. 1, Section 7.6.3.7.2 of proposed SAR, Rev. 1, and Section 2.3.22 of the FRS (Ref. 15), the licensee stated that both ERs rooms are equipped with emergency stop buttons. An emergency stop button is also located on the reactor console. Pressing any emergency stop buttons causes an immediate reactor scram and gives a scram indication to the reactor operator at the control console. To restart operation, the operator must move the console key switch to the RESET position, wait for the time delay to pass, and reset the emergency stop button in the ERs.

Section 2.3.21.4 of the FRS (Ref. 15) states that the cabinet housing the FIS includes large pilot lights provide a visual indication to the operator in the control room of the FIS status. The lights are combined in functional groups, as listed below in Table 2.

Table 2 – FIS Lights

Group	Switches	Function
Interlock position switches	Power On Door No. D1 closed Door No. D2 closed Door No. D2 open Door No. D3 closed Reactor position, fast neutron room Reactor position, thermal neutron room	Indicate status of the limit switches
Reactor operating circuits	Power On Door No. D2 closed Door No. D1 closed Door No. D3 closed Reactor positioned	Operate the reactor
Reactor lead shield door No. 2	Power On Door No. D1 closed Door No. D3 closed Reactor positioned	Operate the lead shield door in the pool
Fast neutron room door No. 1	Power ON Door No. D2 closed Reactor positioned	Operate ER #1 plug door (fast neutron)
Thermal neutron room door No. 3	Power ON Door No. D2 closed Reactor positioned	Operate ER #2 plug door (thermal neutron)
Override switch	Left - Region 1 Center - Off Right - Region 3	Allow movement of the core when not in Region #1 or #3

The licensee stated the function of the override switch in Ref. 4. This switch is used to move the core when it gets stuck between Region 1 and 3, as described in Section 2.3 of the LAR Supplement, Rev. 1 (Ref. 4). This function was previously done manually with potential hazards to the operator.

In addition, the ER includes Exposure Room Status Panel, located between the ERs, to indicate whether it is safe to enter the ER. The status panel has lights to indicate the location of the core, if the lead shield door is open or closed, and if it is permitted to open the ER plug door. The AFRRRI operator would also receive indication of the status of the plug doors since the indication is also displayed on the Left Side Status display on the control console along with the Reactor Mode Control Panel. Furthermore, outside the ERs is the control box for each room. These boxes include the controls to operate the plug doors to enter the ERs. During the audit, AFRRRI demonstrated operation of the control box and the Exposure Room Status Panel.

Interlocks

The FIS uses the state (Open/Close) of the following limit switches to create its interlocks. These limit switches are identified in Figure 7-18 in the proposed SAR Rev. 1. Also, the locations for the different doors are identified in Figure 27 in the LAR. In Table 9 of the LAR

Supplement, Rev. 1 (Ref. 4), provides a cross reference between the terms used in these two figures.

- Plug door open limit switch
- Plug door close limit switch
- Region 1 end stop limit switch
- Entering Region 1 limit switch
- Lead doors close limit switch
- Lead doors open limit switch
- Entering Region 3 limit switch
- Region 3 end stop limit switch
- Plug door open limit switch
- Plug door close limit switch

These signals along with others are used in the logic for the facility interlocks. Section 2.4.1 of the LAR Supplement, Rev. 1 and Section 7.3.5 of proposed SAR, Rev. 1 (Ref. 4) identify the logic and status of each signal to perform these functions. To operate the reactor, the following must be true:

1. The Key Switch must be in the ON position.

AND

2. All emergency stop circuits in the ERs and control system console must be energized.

AND one of the following:

3a. The tank lead shield doors must be fully closed, AND the plug door for the ER against which the reactor is to be operated must be closed, AND the reactor must be in the corresponding region.

OR

3b. The tank lead shield doors must be fully opened, AND both plug doors for the ER rooms must be closed.

The FIS will generate the "Reactor Permissive ROX" signal once all these interlocks are satisfied. This signal is transmitted to the scram loop, and it is part of the magnet circuitry and the transient control rod air circuit.

Lead Shield Doors

LAR Supplement Rev. 1, Section 2.4.2 (Ref. 4) describes the lead doors. The lead shield doors located in the reactor pool and divide the reactor tank in two equal sections. The shield doors, when fully closed, allow access to one ER without significant radiation exposures while experiments are taking place in the other ER. The lead shield doors are provided to reduce exposure from the core in undesired portions of the facility based on the current core location.

These doors include limit switches to indicate when the doors are fully opened or closed. These limit switches, which are part of the FIS, also prevent movement of the core support carriage

into the mid-pool region if the shield doors are opened and prevent power supply to the control rod magnets unless the shield doors are either fully closed or fully opened. The lead shield doors must be fully opened before the core can be relocated. If the reactor tank shield doors are in any position other than fully open or fully closed, a reactor scram will be initiated. During the audit (Ref. 5), AFRRI demonstrated operation of the lead doors. They also demonstrated that for operation of the reactor, the core always needs to be located between the two lead shield doors.

Core Support Carriage

LAR Supplement Rev. 1, Section 2.4.3 (Ref. 4) describes the core support carriage. This equipment was not modified in the LAR. The core carriage includes the reduction gears to provide power to open the lead shield doors. The carriage travels on two tracks that span the reactor tank is used to move the reactor core laterally from one operating position within the tank to another.

The carriage includes limit switches to stop the drive motor when the carriage has reached the length of the track (for both extreme limits of travel). Each region includes the following two limit switches to stop core dolly movement.

- Outer limit switch stops the core dolly when it reaches the far end of the travel to prevent contacting the pool liner. The outer switches cannot be overridden.
- Inner limit switch stops the core dolly from further movement if the lead shield doors are not fully opened to prevent contact with the lead shield doors.

The switches are part of the FIS logic. The licensee stated in Ref. 4 and in Item 9 (Ref. 16) that as part of the LAR, they added a core dolly override switch to the front of the FIS to allow movement of the core dolly when it is stopped in between Regions 1 and 3. The licensee uses administrative control to allow the operator using this override switch.

The operator moves the core carriage from the control console. The carriage position is indicated on the control console.

Plug Doors

LAR Supplement Rev. 1, Section 2.4.4 (Ref. 4) describes the plug doors. These doors provide access to the ERs from the preparation area and prevent radiation streaming from the ERs.

AFRRI's health physics procedures administratively govern the opening of the ER plug doors. The FIS logic must be satisfied for the logic in the ER control boxes allow operation of the plug doors. During the audit, the licensee demonstrated operation of the plug doors.

3.5.1. Technical Evaluation of the Design Bases of the FIS

The FIS consists of a series of limit switches and pushbuttons to implement a logic to prevent opening or closing of the reactor tank shield doors and to prevent the movement of the reactor core between different regions unless specific conditions are satisfied. In this manner, the FIS will eliminate the possibility of accidental radiation exposure of personnel working in the exposure rooms and prevent interference between the reactor tank lead shield doors and reactor core shroud. Further, the FIS is designed to prevent inadvertent operation of the reactor

when the conditions of all interlocks have not been met. All of the interlocks are binary (on/off and open/closed).

The FIS logic uses signals from status of core position, reactor tank shield doors, ER, plug doors, and physical movement of the reactor. Also, the FIS interfaces with the console magnet power key switch to enforce its logic. The signal from the magnet power keyswitch is part of the FIS logic, and it should be in the "ON" position for the logic to function. Once the interlocks are satisfied, the reactor permissive (ROX) relay associated with the FIS in the scram loop will energize and start a delay timer, so the magnet circuitry can be energized. Section 7.3.5 of the proposed SAR Rev. 1 (Ref. 4) describes the steps to energize the magnet circuitry. During the audit (Ref. 5), the licensee demonstrated the operation of the magnet key switch, located on the rod control panel, to energize the magnet circuitry.

The FIS components were designed to fail-safe. If any of the limit switches fail, they will default to their safe state of an open circuit and thereby prevent facility operation. During the audit, the NRC staff reviewed wiring diagrams, operation manuals, and tests performed to demonstrate the operation of the FIS and the magnet circuitry.

The FIS is installed in a stand-alone cabinet, which includes pilot lights in the front. These lights are in functional groups to provide a visual indication to the operator in the control room of the FIS status. The lights would illuminate when the logic necessary is satisfied. During the audit (Ref. 5), the NRC staff visually confirmed the location and operation of these lights.

The FIS components are commercial grade analog devices. The licensee performed rigorous testing and quality assurance at multiple steps in the FIS design, manufacture, and installation process. During the audit, the NRC staff reviewed the acceptance tests for the FIS, as well tests performed during factory acceptance and site acceptance test of the I&C system.

The ER includes control boxes and status panel. The control boxes include the logic necessary to operate the plug doors. The status panel will indicate the status in the ERs and show the operator if it is safe to enter. Inside each ER, a control panel is installed, which includes the emergency stop pushbutton, a horn, and the horn bypass switch. The horn will sound for 30 seconds when the reactor is about to start operation. The bypass switches can silence the horn when performing noise sensitive experiments. The emergency stops prevent accidental radiation exposures in each ER. During the audit, after following the appropriate AFRRRI procedures, the NRC staff entered ER #1 to confirm location of the local panel.

3.5.2. Technical Evaluation of the Design Criteria

This section of the SE documents the NRC staff's review and evaluation of the proposed FIS design to perform its safety functions based on the appropriate design criteria to satisfy the 10 CFR 50.34(a)(3) and (b) requirements. The NRC staff's evaluation of the design of the proposed scram loop is based on acceptance criteria in Sections 7.2 and 7.3 of NUREG-1537, Part 2.

The licensee identified the design criteria for the scram loop in Section 2 of the LAR Supplement, Rev. 1 and Section 7.3.5 of the proposed SAR, Rev. 1 (Ref. 4).

(a) Single failure

The FIS consists of limit switches to perform a logic table to allow the movement of the reactor. The FIS components were design to fail-safe. If any of the limit switches fail, they will default to their safe state of an open circuit and thereby prevent facility operation

(b) Independence

Section 7.4 of NUREG-1537, Part 2, states that the SAR should address the separation and independence of the RCS and RPS and show independence of detector channels and trip circuits.

The FIS is not completely independent from the RPS because the scram loop contains the ROX, which is a relay actuated by the FIS. However, the configuration for interactions between the systems ensures any malfunction in the FIS will not prohibit the protection functions of the RPS. Since the relays in the scram loop are in series, a failure of the FIS will not prevent any of the remaining RPS relays from opening and causing the reactor to scram. As discussed in Section 3.5.1 of this SE, the logic in the FIS must be satisfied to operate the reactor. Consequently, the FIS provides a diverse and independent method that will scram the reactor if the limit switches are de-energized.

(c) Fail-safe on Power loss

As described in Section 3.1 of this SE, the CSC includes an uninterrupted power supply (UPS), which is connected to the offsite AC power. The LAR Supplement, Rev. 1, Section 1 and Section 7.2.1 of the proposed SAR, Rev. 1 (Ref. 4) describe the distribution of AC power from the UPS to the DAC and then to components housed within the DAC. Section 3.1 also explains that if external power is lost, the UPS will initiate a scram, and provide power to the console for approximately 15 minutes to allow the operator to gracefully shutdown the console. The UPS is not a safety-related system, and it is not required to power any safety systems. Therefore, a loss of electrical power or multiple circuit damage due to a fire, explosion, dropped load, or some other cause will result in the limit switches deenergizing and opening the permissive relay in the scram loop.

(d) Effects of Control System Operation/Failures

The FIS consists of limit switches to implement a logic table to operate the reactor. The FIS also provides a permissive for the magnet circuitry to energize. These limit switches receive signals from the core position, reactor tank shield doors, ER, plug doors, and location of the reactor.

(e) Bypass, Permissives and Interlocks

There are no means for the reactor operator to manually bypass any limit switches in the FIS.

The FIS logic energizes the ROX relay, which it is part of the scram.

The signal from the magnet power keyswitch is part of the FIS logic, and it should be in the "ON" position for the logic to function.

The ERs include bypass switches to silence the horn when performing experiments sensitive to noise.

(f) Surveillance

In the proposed LAR and SAR (Ref. 4), the licensee stated that the current surveillance requirements remain unchanged. The TS are evaluated in Section 3.11 of this SE.

(g) Quality

The licensee replaced FIS components, such as wiring, relays, limit switches, pushbuttons, etc., with new readily available functionally equivalent commercial off the shelf (COTS) components. In the SAR and LAR (Ref. 4), the licensee stated that they performed rigorous testing and quality assurance at multiple steps in the FIS design, manufacture, and installation process. During the audit (Ref. 5), the NRC staff reviewed test documents for the FIS, including the acceptance test, FAT, and SAT. In addition, the NRC staff reviewed quality documents and procedures utilized by the vendor of these components. Section 3.10 of this SE provides the NRC staff's review of the quality process, development, and testing for FIS.

Based on its review of the information provided above and the discussion in Section 3.10 of this SE, the NRC staff finds the FIS was developed in accordance with the vendor's QA plan and procedures and properly documented and certified by the licensee. The NRC staff also finds that the licensee followed the ANSI/ANS-15.8-1995 guidance to identify, follow, and document applicable design inputs, such as design bases, performance requirements, regulatory requirements, codes, and standards. The NRC staff concludes the design of FIS meets this criterion and is acceptable.

Based on the evaluation of the information presented above, the NRC staff concludes FIS interlocks are consistent with the guidance in NUREG-1537, Part 2, and prevent the operation and movement of the reactor core into an area until assurance is provided that inadvertent exposure will be prevented.

3.6. Reactor Protection System

The RPS monitors variables to safely operate the reactor. In case that monitored variables exceed their limits, the RPS will scram the reactor and maintain the facility in a safe condition. The RPS mainly comprises the scram logic circuitry. Section 7.4 of the SAR, Rev. 1 (Ref. 4) identifies the process variables monitored, which are neutron flux, fuel temperature, and coolant level. In addition, the RPS receives signals from the CSC, manual scram, magnet power key switch, loss of power, and emergency stops in the ERs. The RPS does not receive signals from the radiation monitoring system (RMS). The operator can monitor data from the RMS in the auxiliary console, located in the control room. The licensee did not request modifications to the RMS and auxiliary console in the LAR.

3.6.1. Scram Loop

In response to a manual or automatic safety signal, the scram loop will de-energize the magnets for the control rods and the solenoid for the transient rod air, which will cause insertion of the control rods into the core, shutting down the reactor. The scram loop is installed inside the DAC with the exceptions of the manual scram pushbutton.

Section 1.6 of the LAR Supplement, Rev. 1 and Section 7.4 of the proposed SAR, Rev. 1 (Ref. 4) describe the proposed scram loop. This section of the SE describes the scram loop and its technical evaluation.

The scram loop consists of a constant current power source that is wired through several relays connected in a loop. When abnormal reactor operating conditions occur or a manual scram is activated, the corresponding relays will de-energize, opening the contact for the relay and breaking the loop. After a delay of about 25 milliseconds (for the magnetic field to decay), the magnets release the control rods and the solenoid for the transient rod air to de-energize which scrams the reactor. The reactor can also be scrammed by turning the magnet power key switch to the OFF or RESET positions. To perform a fast scram, the operator can use the manual scram push button.

The AFRRRI design criteria for its I&C system requires reactor scram to prevent exceeding the safety limit for operation. AFRRRI identified the following design basis events, for which safety scrams are included in the loop:

- the operation of the reactor at a steady-state power level in excess of the corresponding technical specification.
- the insertion of reactivity which causes the reactor to exceed the temperature limit during a pulse.

Parameters monitored for this purpose include neutron flux, fuel temperature, coolant level, area radiation, and the release of radioactive materials. Table 8 in the LAR (Ref. 4) lists all scram contacts in the scram loop.

The SAR and LAR (Ref. 4) identified 3 external signals (EXT1 – EXT3) and the NPM-1000 (loss of HV and overpower trips) that are not used. These signals are jumpered out in the DAC. The DAC is locked, and it is not easily accessible to the staff to modify. The licensee checks signal configurations as part of calibration and surveillance of the scram loop.

3.6.2. Technical Evaluation of the Design Bases of the Upgrade of the RPS

This section of the SE describes the NRC staff's evaluation of the design basis of the upgrade of the RPS using the design bases acceptance criteria of Section 3.1 and 7.4 of NUREG-1537, Part 2.

Sections 7.4.1 and 7.4.2 of the proposed SAR, Rev. 1 (Ref. 4) identifies the design bases and criteria used for the upgraded scram loop. The principal design criteria of AFRRRI establishes the necessary design, fabrication, construction, testing, and performance requirements for structures, systems, and components important to safety that provide reasonable assurance that the TRIGA reactor can be operated without undue risk to the health and safety of the public. The regulations in 10 CFR 50.34(a)(3)(ii) require the applicant to describe the design bases and the relation of the design bases to the principal design criteria. Section 50.34(b) of 10 CFR

requires updating the information that takes into account any pertinent information developed since the submittal of the preliminary SAR.

The NRC staff's design basis evaluation reviews the adequacy of the protective system design to monitor the parameters that detect the need for protective action and perform its protective function. The principal design action of a protection system is to rapidly place the reactor in a subcritical condition by automatically inserting the control and safety rods whenever any of the selected parameters exceeds predetermined limits.

The scram loop is part of the Reactor Protection System, and as such it will provide protection to the reactor before any safety limits are reached. The scram loop uses signals from multiple measurements of the power level, fuel temperature, pool water level, high voltage loss of the neutron flux, manual scram button, and console key. The scram loop also includes digital signals generated by the CSC computers (i.e., software).

All scram inputs to the scram loop relays are from independent channels. Further, there is no voting among the channels to de-energize a relay and scram of the system. Any single parameter that is outside of the normal operating range will cause a scram. Also, when AC power is lost, the UPS will generate a scram signal and supply power to the control console for the operator to monitor instruments and shutdown the console.

LAR, Supplement, Rev. 1 (Ref. 4) includes Figure 23 which shows the scram loop and its components. The scram loop consists of:

- K1
- K2
- Scram loop relays

The K1 performs the reset and latching functions, indicates all SCRAMs clear, and completes the circuit that enables the transient rod air solenoid to be activated. The K2 relay is energized when the console key switch is in the ON position and provides the operate signal for the Facility Interlock System.

When a scram is initiated, magnet power is removed (and transient rod air pressure removed) and the control rods fall into the core under the force of gravity. The shim, safety, regulating, and transient rod drive motors all drive to the bottom limit switch after a scram. The scram circuits and components are completely hardwired and do not in any way depend on the CSC computers or any software to perform a scram. Furthermore, the reactor operator has no capabilities to bypass the scram relays so that the reactor can be operated at conditions that are beyond the limits defined by the trip set points. These relays are inside the DAC, which is locked and is not easily accessible to the AFRR staff.

Power level scrams ensures the reactor will be shutdown prior to the fuel temperature safety limit being exceeded. In the steady-state mode, the two channels that perform the high-power scrams are the NP-1000 and NPP-1000. In pulse mode, only the NPP performs a high-power scram, and the NP scram contacts are temporarily bypassed as stated in Item 3 (Ref. 16).

The neutron flux detectors rely on a high voltage differential to perform their measurement function. If the high voltage drops significantly, their ability to detect neutrons is inhibited and will result in an underestimation of the neutron flux within the core. Therefore, a loss of high voltage to any of the detectors for high flux safety channels will cause a reactor scram.

After a scram is initiated, the LATCH contact is designed to permanently de-energize the loop after a scram has occurred. To reset the loop and energize the standard control rod magnet power circuits and the transient control rod air circuits, the reactor operator must clear all scrams and place the Magnet Power Key Switch to the Reset position. Also, all interlock permits must be satisfied. Sections 1.6.4.1 and 7.3.5 of the LAR/SAR, respectively (Ref. 4) describes the operation of the key switch. Further, during the audit (Ref. 5), the NRC staff observed operation of the key switch.

Section 7.1.1 of the proposed SAR, Rev. 1, states that the time from initiation of a scram to full insertion of the rods is less than one second.

The scram loop design includes independence (of the safety channels) and diversity to protect against common cause failures. Further, if a common cause failure occurs, this failure cannot prevent the system from shutting down the reactor because the system is designed to be fail-safe. A loss of power, a component failure, circuit damage due to external hazards (e.g., fire), or some other cause will result in a loss of power to the magnets that connect the control rods and control rod drives, causing the control rods to drop into the core.

The scram loop also includes a software generated scram signal and two CSC-timed scrams. The "Software" input in the scram loop is generated by the CSC computer when its digital I/O module communication is interrupted. Also, this scram will be generated when the magnet power key switch is turned to the OFF position.

The CSC includes two timed scrams in the scram logic, which are steady-state timer and pulse timer. These timed scrams are used for experiments which need a predetermined exposure time and these timed scrams are used to ensure a pulse does not create excessive energy within the fuel. The steady-state timer causes a reactor scram after a predetermined elapsed time. The reactor operator selects the time on the control console during steady-state power operations. During a run, the timer may be started and stopped by the operator. The pulse timer causes a reactor scram when in pulse mode. The timer may be set for a duration shorter than 15 seconds. However, the console will automatically initiate a scram timeout after 15 seconds. The CSC also controls three additional relays: SHIM MAG, SAF MAG, and REG MAG. These relays are designed to activate and deactivate magnet power to individual rods.

The scram loop includes relays associated with the doors in the ERs to prevent accidental radiation exposure. These relays are tied to emergency stops provided in each ER. Additionally, the control console includes an emergency stop switch for the operator to stop door motion and core motion. The emergency stop switch and/or emergency stops will initiate a reactor scram and give scram indication to the operator on the console. Whenever the operator uses the emergency stop switch, this switch must be cleared by turning the key switch to reset. If the emergency stop was initiated from one of the ERs, the local switch must also be reset by manually pulled the switch out to permit operation. Once the reset is activated, the horns in the ERs will activate again with the associated time delay. This reset is required to initiate magnet power and begin inserting reactivity to the core.

3.6.3. Technical Evaluation of the Design Criteria

This section of the SE documents the NRC staff's review and evaluation of the proposed scram loop design to perform its safety functions based on the appropriate design criteria to satisfy the 10 CFR 50.34(a)(3) and (b) requirements. The NRC staff's evaluation of the design of the

proposed scram loop is based on acceptance criteria in Sections 7.3 and 7.4 of NUREG-1537, Part 2.

The licensee identified the design criteria for the scram loop in Section 1.6 of the LAR, Supplement, Rev. 1 and Section 7.4.1 of the proposed SAR, Rev. 1 (Ref. 4).

(a) Single failure

The scram loop includes several independent relays, configured to scram the reactor independently from each other. Each individual component will cause a scram regardless of the status of any other relay or system. Therefore, a single failure of any relays would not prevent the scram loop from functioning as expected. When a signal to open a relay is received or when loss of power occurs, or failures affect scram loop components, the scram loop will shutdown the reactor.

All scram capability is built in series allowing for any single system to initiate reactor shutdown. This eliminates the possibility of systematic, non-random, concurrent failures of redundant elements in the protection systems and reactivity control systems. In addition, the CSC includes logic to detect I/O communication failure, computer failure, and power supply failure. The CSC also includes a watchdog timer to ensure the control console remains responsive. The failure of any of these components will generate a signal to scram the reactor. In this manner, the CSC provides a higher level of safe operation.

During the audit (Ref. 5), the NRC staff reviewed the scram loop and magnet power circuitry and confirmed that all signals identified in the LAR will interrupt power to the magnet circuitry, causing the reactor to scram.

Based on this information provided and reviewed, the NRC staff finds that the scram loop will perform its protective action by interrupting power to the magnet circuitry. In addition, the NRC staff finds that the design of the scram loop includes multiple, diverse ways to initiate a reactor scram when the failure of any single component or channel occurs. Therefore, the NRC staff concludes that the proposed scram loop will perform the required protective actions in the presence of any single failure or malfunction and meets the design acceptance criterion in NUREG-1537, Part 2, for single failure and the design acceptance criteria in Sections 5.1 and 5.4 of ANSI/ANS-15.15-1978 for single failure and fail-safe.

In addition, because the scram loop design includes diverse ways to initiate a reactor scram and perform its safety function, it meets the design acceptance criteria in NUREG-1537, Part 2, which establishes that the system's design features should be sufficient to protect the health and safety of the public.

(b) Redundancy

Standard criteria for the design of a nuclear facility are the application of redundancy and diversity to address single failures. This practice is achieved in the scram loop by having multiple instruments measuring parameters throughout the operating range of the facility. The operation of the AFRR1 TRIGA reactor requires at least two operable channels for all steady-state modes of operation, as identified in TS 1.6.6. Because the fuel temperature is the primary reactor parameter to be protected, there are at least two

fuel temperature safety channels operable for all modes of operation. Therefore, multiple measurements of the power level and the fuel temperature are made by independent channels with different detection mechanisms (fission chambers, ionization chambers, and fuel temperature monitoring).

The scram loop system design uses redundant relays from different and independent systems to shut down the reactor. In this manner, if one relay fails to scram the reactor, others can scram the reactor. The relays can be activated or deactivated by the neutron and fuel temperature monitors, low pool level.

In addition, the CSC includes logic to detect I/O communication failure, computer failure, and power supply failure. The CSC also includes a watchdog timer to ensure the control console remains responsive. The failure of any of these components will generate a signal to scram the reactor. In this manner, the CSC provides a higher level of safe operation. Note that this is a redundant feature. When the hub loses communication with the computer, it will put all relays in a fail-safe state, thus scrambling the reactor. It also deactivates when the magnet power key switch is turned to the RESET position, thus scrambling the reactor.

In addition, AFRR1 includes manual actuation devices for the operator or staff to shut down the reactor if all automatic protective means were to fail. These manual devices include ones in which the operator can depress the manual scram buttons, remove the key switch on the control console, depress emergency stops in ERs or emergency stop switch in the control console. Any of these manual devices will interrupt power to the magnet circuitry and scram the reactor.

During the audit (Ref. 5), the NRC staff reviewed the magnet power circuitry and confirmed that redundant signals from different systems and manual actuation devices will interrupt power to the magnet circuitry, causing the reactor to scram.

The AFRR1 facility includes redundant indications of reactor power and change rate in the control console and the analog bargraphs, and the indications are monitored by the CSC to ensure they remain in the expected range.

Based on the information provided, the NRC staff finds the scram loop design includes redundant and diverse ways to initiate a reactor scram and perform its safety function. Further, the scram loop meets the design acceptance criteria in NUREG-1537, Part 2, which establishes that the system's design features should be sufficient to protect the health and safety of the public.

(c) Independence

The scram loop consists of relays connected in series, allowing for any single system to perform a complete system scram. The systems or devices generating the signals for these relays are independent from each other and do not depend on obtaining information from any other systems to scram the reactor. Each of the neutron channels and fuel temperature channels will operate independently. In addition, each neutron channel and fuel temperature channel have dedicated cabling to and from the measurement detector to the channel and there is no connection between channels. Therefore, scram capability by each channel is accomplished by each channel individually and for each parameter (neutron flux, power level, fuel temperature)

measured. Further, the detectors are in various locations around the core, providing independent reading for each parameter. Because the neutron flux is spatially dependent, at least two detectors are on range at any steady-state operating power value. These detectors are located around the core to prevent inaccurate indication from phenomena such as rod shadowing and flux tilt.

Analog signals transmitted to the neutron and fuel temperature monitors are divided and transmitted to the operator console and to the bargraphs. Therefore, if the CSC does not receive these analog signals, the scram loop will continue to perform its safety function.

The scram circuits and components are completely hardwired and do not depend on the CSC computers or any digital system to perform a scram. The CSC includes signals in the scram loop, but these are independent from all other signals in the scram loop. These signals are part of the CSC logic to generate a scram signal, and consequently interrupt power to the magnet circuitry causing the reactor to scram. This configuration will not prohibit the protection functions of the RPS. Since the relays are in series, a failure of the CSC relay will not prevent any of the remaining RPS relays from opening and causing the reactor to scram. The safety functions for the AFRRI TRIGA reactor are all analog and do not depend on the computer system. Further, the licensee does not credit the CSC relay for safe shutdown of the reactor. However, it provides a diverse and independent method to scram the reactor. In case that erroneous indication is transmitted to the control console, the operator can crosscheck this information with the data transmitted to the recorders and bargraphs, which is independently transmitted from the NIs.

The scram loop was designed such that it can perform its entire functionality without interaction from the operator. Further, the CSC has no means to modify the configuration of the scram loop, neutron and fuel temperature channels, or low pool level detector. Modifications to the neutron and fuel temperature channels can only be performed in these channels, as described in Section 3.3 of this SE.

The scram loop receives power from the DAC, which gets power from the UPS. The UPS unit provides power to the control console during normal operation. During the loss of AC power, the magnet circuitry will open and initiate a scram and the UPS unit will power the control system for operators to monitor reactor conditions and perform an orderly shutdown of the console computers. During the audit (Ref. 5), the NRC staff observed that the logic in the CSC to scram the reactor includes a signal associated with loss of AC power supply, which will generate the UPS Power Loss scram signal and provide sufficient power for the CSC. Although all systems rely on the same source of power, all instruments are independent from each other and in the event of loss of AC power, the scram loop will shut down the reactor.

The scram loop is housed in the DAC, along with reactor instruments and certain control systems. Thus, cables for protection and control of the reactor run side by side. The DAC is installed in the reactor room. Although many safety instruments and control systems are installed in the DAC, the DAC was designed so that in the event of a channel failure, a scram will be automatically initiated, and the reactor will shutdown. Further, the licensee stated in Section 7.4.3 of the proposed SAR, Rev. 1 (Ref. 4), that in the event of loss of power or multiple circuit damage due to a fire, explosion, dropped load, or some other cause, the result will be that the circuit magnetry loses power,

shutting down the reactor. This ensures a fail-safe design of the scram loop, even when the components are housed in the same location. The control console is installed in the control room, which is physically separated from the reactor room.

During the audit (Ref. 5), the NRC staff reviewed RPS's documents and engineering drawings to confirm the physical, electrical, and communication independence between the RCS and the RPS. These documents and drawings show they are sufficiently independent to preclude any interactions which would result in the compromising of the function of the safety system. The NRC staff confirmed that the neutron channels provide input to both the control console and the RPS. The NRC staff also confirmed that the neutron and fuel temperature monitoring signals transmitted to the CSC for monitoring and operation are isolated in the DAC via air gapped Ethernet communication. Although the cabling is in the same cabinet and routed together, separate cables carry the signals to the RCS and RPS.

Based on the information provided, the NRC staff finds that the scram loop is sufficiently independent from control and auxiliary systems, the scram loop design includes sufficient and diverse means to protect the reactor when the failure of any single component or channel occurs. Therefore, the NRC staff concludes that the proposed scram loop meets the intent of the acceptance criteria for independence for the failure of any single component or channel in NUREG-1537, Part 2.

(d) Defense-in-Depth

The scram loop design includes independent (of the safety channels) and diverse channels to scram the reactor. The scram loop includes signals from the neutron monitors and fuel temperature monitors, manual devices to scram the reactor (e.g., key magnet switch), software-generated scrams, low pool level, UPS, reactor permissive, emergency stops, pulse and steady-state timers, and magnet power key switch.

The scram signals associated with the fuel temperature monitors (NFT-1000) will maintain the safety limit, as defined in the AFRRI TSs. Further, the power level scrams ensure the reactor can be shutdown prior to the fuel temperature safety limit being exceeded. In the steady state mode, the two channels to perform the high flux scrams are the NP-1000 and NPP-1000.

The RCS and RPS are not completely independent because the scram loop contains a relay that is actuated by the RCS. However, their signals are configured in such a way there is no possible interactions between them. In this manner, the systems design ensures that any malfunction in the software scram relay generated by the RCS will not prohibit the RPS from performing its protection functions. Since the relays are in series, a failure of the RCS relay will not prevent any of the remaining RPS relays from opening and causing the reactor to scram. Further, the licensee does not credit the RCS relay for protection and safe shut down of the reactor. However, it provides a diverse and independent method to scram the reactor.

The AFRRI reactor requires at least two operable channels for all steady-state modes of operation, as identified in TS 1.6.6. Therefore, multiple measurements of the power level and the fuel temperature are made by independent channels with different detection mechanisms (fission chambers, ionization chambers, and fuel temperature

monitoring), and these multiple measurements provide defense-in-depth to protect the reactor.

The CSC includes logic to detect I/O communication failure, computer failure, and power supply failure. The CSC also includes a watchdog timer to ensure the control console remains responsive. The failure of any of these components will generate a software-generated signal to scram the reactor. The use of multiple ways to shut down the reactor provides defense-in-depth to ensure the integrity of the reactor.

The AFRRI facility includes manual devices (or switches) for the staff to scram the reactor. Different push buttons are provided in the ERs to prevent accidental radiation exposure and initiate a reactor scram. The emergency stops provided in each ERs have a relay in the scram loop. Additionally, the control console includes an emergency stop switch for the operator to stop door motion, core motion, and initiate a reactor scram.

Based on the information provided, the NRC staff finds that the scram loop design includes different mechanisms to scram the reactor, providing defense-in-depth to protect the reactor and to ensure that the safety limit is not exceeded. Further, the use of defense-in-depth measures ensures that the reactor can be safely operated and shutdown without posing undue risk to the health and safety of the AFRRI staff or environment. Therefore, the NRC staff concludes that the proposed scram loop meets the intent of the acceptance criteria for the failure of any single component or channel in NUREG-1537, Part 2.

(e) Reliability

Table 1 of the LAR, Rev. 1 (Ref. 4) identifies the components for the scram loop. These components are:

- Omega OME-DBRD Relay Board
- Fujitsu RY Series Electromechanical Relays
- COTS I/O Boards
- IDEC RHIB-U-DC24V Electromechanical Relays
- Allen Bradley 700-HC24Z24
- Electromechanical Relays (K1 & K2) - identical 4PDT, 14 blade, 24 Vdc, ice cube type relays.

The relays for the scram loop are all commercial, Form C electromechanical relays mounted on a PWA (printed wiring assembly) board. A total of 24 relays are installed on the board, although not all are currently being used. The relays EXT1, EXT2, and EXT3 are not connected and the HV and %pwr contacts of the NMP-1000 are jumpered out.

Because the components are not nuclear grade, a documented process was used to test, verify, and validate that the scram loop is robust and reliable to perform its functions. During the audit (Ref. 5), the NRC staff reviewed the vendor's software development plan, quality assurance program, and tests performed to demonstrate proper installation and operation of the relays. The NRC staff confirmed that these components can perform their functions during normal and abnormal conditions. Based on this information, the NRC staff concludes that the scram loop is reliable and robust to perform its functions.

As described above, the scram loop was designed considering features that can improve its reliability. In this case, AFRRRI considered independence, redundancy, diversity, maintenance, testing, and quality components as part of the scram loop design. These features were described and evaluated in items (a) through (d) and (f) of this section.

Based on the information reviewed, the NRC staff finds that the scram loop was built of high-quality components using accepted engineering and industrial practices, and the system was tested to demonstrate proper operation. Therefore, the NRC staff concludes that the proposed scram loop meets the intent of the acceptance criteria for using reliable components in NUREG-1537, Part 2.

(f) Fail-Safe

Each individual component will cause a scram regardless of the status of any other module. The scram loop design incorporated the principle of fail-safe by allowing any one system to initiate protective action. There is no voting or other logic whereby communication between channels is required to protect the reactor.

The scram loop includes the LATCH contact, which is designed to permanently de-energize the loop after a scram has occurred. This contact is part of K1. The loop will stay de-energized until the operator places the Magnet Power Key Switch to the Reset position. Further, the reactor cannot be restarted until the trip state is cleared, the operator places the Magnet Power Key Switch to the Reset position, reactor permissives and shield door movement circuits are satisfied, and K1 has been successfully reset and indicates ALL SCRAMS CLEAR. During the audit (Ref. 5), AFRRRI could not manipulate the controls of the reactor because it directly affects reactivity. To accomplish this, AFRRRI staff pulled out the K1 relay, which performs the reset and latching functions and indicates all SCRAMS clear for the scram loop.

The scram loop also includes a signal to alert the operator when a ground fault is detected. Further, the neutron channels include a high voltage trip that will scram the reactor when the voltage is below a defined setpoint. The high voltage value is displayed on the local instrument, but a low-HV trip is displayed on both the local instrument and at the control console.

The AFRRRI facility includes manual devices (or switches) for the staff to scram the reactor. Different push buttons are provided in the ERs to prevent accidental radiation exposure and initiate a reactor scram. The emergency stops provided in each ERs have a relay in the scram loop. Additionally, the control console includes an emergency stop switch for the operator to stop door motion, core motion, and initiate a reactor scram.

To protect the reactor and prevent radiation exposure in the reactor room, the pool water includes a level switch, which will activate if the water level drops below 14 feet from the top of the core. If the switch is activated, its scram relay will open, interrupting power to the magnet circuitry and shutting down the reactor.

Based on the information reviewed, the NRC staff finds that the AFRRRI fail-safe design meets the accepted engineering and industrial practices, and the system was tested to demonstrate proper operation. Therefore, the NRC staff concludes that the proposed

fail-safe design meets the intent of the acceptance criteria for using reliable components in NUREG-1537, Part 2.

(g) Protection system operation/failures

When a limit or setpoint is exceeded, the corresponding signal will scram the reactor. In addition, there are manual devices (e.g., scram push button) to shut down the reactor. The scram is achieved through both the removal of magnet power to the standard rod drives and the removal of air pressure to the transient rod. Upon removal of magnet power and air pressure, the rods fall into the core due to the force of gravity.

In Section 7.1.1 of the SAR Rev. 1 and AFRRRI TS 3.2.1 (Ref. 4), the licensee stated that the time from initiation of a scram to full insertion of the rods is less than one second. The licensee verified this time during the SAT, which the NRC staff reviewed during the audit (Ref. 5).

Based on the information reviewed, the NRC staff finds that the AFRRRI protection system operation/failures design meets the accepted engineering and industrial practices, and the system was tested to demonstrate proper operation. Therefore, the NRC staff concludes that the proposed protection system operation/failures design meets the intent of the acceptance criteria for using reliable components in NUREG-1537, Part 2.

(h) Setpoints

The licensee did not modify previously approved TS values for the SL or LSSS in the LAR. The safety limit is a fuel temperature of 1,000°C, which is measured by three thermocouples in the reactor and three independent processing units of the NFT-1000 to monitor and protect the fuel temperature. In Section 7.4.4 of the SAR, the licensee described how the NFT-1000 setpoint was determined.

The methodology used by the licensee to determine reactor power and neutron flux setpoints were not reevaluated by the NRC staff. Section 3.3.5 of this SE describes and evaluates the NFT, as well as the setpoint setting.

Section 7.3.6., TS 3.2.1.c, Table 1, Notes 1 and 2, describe the process for when channels become inoperable.

Reactor power values are indicated in three locations for the operator. The first location is on the front panel of the neutron flux and fuel temperature channels. The second is in the control console where operators can monitor these values. Third, analog signals from the neutron and fuel temperature channels are sent to bargraphs and recorders in the control room.

During the audit (Ref. 5), the licensee demonstrated the use of the control console, bargraphs and recorders for indications for the neutron and fuel temperature channels and plant parameters. The NRC staff observed how the licensee can retrieve setpoint values and how authorized personnel could modify these setpoints to validate the information contained in the LAR.

Based on the information provided and reviewed, the NRC staff finds that the proposed I&C systems and subsystems will measure the parameters necessary to protect the reactor, and the previously approved setpoints will continue to protect the fuel and help ensure public health and safety. Therefore, the NRC staff finds that the proposed I&C systems meet the acceptance criteria for setpoints, accuracy requirements, and actuated equipment response time in Section 7.4 of NUREG-1537, Part 2 and Section 5.6 of ANSI/ANS-15.15-1978 to assure that the proper setpoints are automatically made active and the system has features that facilitate administrative controls to verify the proper setpoints.

(i) Bypass/permisives and interlocks

TS 3.2.2 identifies the reactor safety system interlocks required during steady-state and pulse mode. These interlocks should be active for the reactor to operate in these modes. The licensee did not modify this table, nor change the interlocks.

The control rod includes an interlock to prevent the movement of the control rods from their inserted core position in the upward direction under the conditions defined in Section 7.3.4 of the proposed SAR (Ref. 4). This interlock will ensure that when operating in pulse mode, the fuel element temperature won't exceed the safety limit, since the NP-1000 scrams are temporarily bypassed. Further, the control rod drive mechanisms include a 3-second period interlock to minimize the possibility of exceeding the SL for the fuel temperature, as described in Section 1.7.5 of the LAR.

In Ref. 16, the licensee described the inhibit signal generated by the RCS when the reactor is in Pulse mode. As described in Section 3.6.2 of this SE, in pulse mode, only the NPP-1000 performs a high-power scram, and the NP-1000 scram contacts are temporarily bypassed. The console display will show the NP-1000 bypassed, NMP-1000 and NLW-1000 inhibited fields.

In Section 7.7.3.2 of the SAR and Section 1.8.1 of the LAR, the licensee noted that an interlock associated with the demineralized water inlet temperature will prevent withdrawal of the control rods if the temperature is greater than 60°C. In Section 7.3.3 of the SAR and Section 1.8.2 of the LAR, the licensee described that a level switch provides an interlock to prevent the withdrawal of the control rods when the level is 1 in. below full pool level.

In Section 7.1.1 of the proposed SAR, the licensee stated that during operations of the TRIGA reactor, the design of the scram loop does not include means to bypass the trips. In the event of a system anomaly or instrument failure, no bypass or interlock will preclude the reactor from being safely shutdown. During the audit (Ref. 5), the NRC staff confirmed that the scram relays cannot be bypassed. Also, the relays are installed inside the DAC, which is locked and not easily accessible to the operators.

In the LAR, the licensee stated that the scrams generated by the NP-1000, NPP-1000, and NFT-1000 cannot be bypassed by the operator. In this manner, reactor cannot be operated beyond the limits defined in the technical specifications and safety analysis report. Except for operation of the reactor in pulse mode, in which the NP-1000 is bypassed. In this case the NPP-1000 scales itself for pulse mode and NFT-1000 remains available to scram if high temperature is reached during pulse. The NLW-1000 monitor includes an interlock at 1 kW for when the reactor is operating in pulse mode.

The AFRRRI facility includes a FIS, which is designed to prevent inadvertent operation of the facility when a set of conditions have not been met and thus eliminate the possibility of accidental radiation exposure of personnel. The reactor control panel includes an emergency stop button, which is included in the FIS. The FIS interfaces with the console Magnet Power keyswitch to enforce its logic. The FIS interlock permits must be satisfied, so the input to the scram loop can be satisfied and the control rod magnet and air circuits can be energized in accordance with AFRRRI procedure. Section 3.5 of this SE describes the FIS. The FIS includes switches from the ERs to silence the horns in these rooms during experiments that are sensitive to noise. Section 2.4 of the LAR states that bypassing these horns should be done in accordance with AFRRRI administrative procedures.

The left-side status pane in the control console includes the INTERLOCK pane to display all interlocks. The right-side pane will also display interlock messages in the annunciator box.

During the audit (Ref. 5), the NRC staff reviewed documents associated with the scram loop, rod withdrawal permissive, and FIS to confirm the information provided in the LAR regarding permissives and interlocks. The NRC staff observed that the interlocks and permissives and interlocks in the FIS and the rod withdrawal do not interfere with the RPS.

Based on its review, the NRC staff finds the design properly documents permissive, interlocks and bypass conditions and appropriate indications are provided. Further, the NRC staff finds that the proposed scram loop do not contain bypasses or means to deliberately induce inoperability of its safety function. Accordingly, the NRC staff concludes that the proposed scram loop for meets the design acceptance criteria for bypass/permissives and interlocks identified in NUREG-1537, Part 2 and Section 5.7 of ANSI/ANS-15.15-1978 and is acceptable.

(j) Completion of protective action

As described in Section 3.2.6.1 of this SE and in Section 1.6 of the LAR, when a scram is initiated, magnet power is removed (and transient rod air pressure removed) and the control rods fall into the core under the force of gravity. The shim, safety, regulating, and transient rod drive motors all drive to the bottom limit switch after a scram. There is no mechanism to prevent the rods from falling all the way into the core; the scram goes to completion once initiated.

The scram loop only performs the function of scrambling the reactor when a signal to open a relay is received, when loss of power occurs, or failures affect scram loop components. Because of this simple design, the scram loop will ensure that the reactor remains safe under all off-normal and accident conditions. Once the actions initiated by the RPS cannot be impaired or prevented by manual intervention, and no manual actions are necessary within a short time to supplement the RPS actions. Also, the actions initiated by the RPS are not self-resetting. The reactor operator must clear all scrams before reactor operation can be resumed. In order to restart the reactor after a scram, the rod drives must be driven to their lower limits (i.e., fully inserted), the magnets re-engaged, and the rods lifted again.

In addition, in Section 1.6.4.3 of the LAR states that when any of the scram loop contacts open, power to K1 is lost, and the coil is de-energized. All K1 contacts then default to the normally open position, permanently interrupting loop current until a Magnet Key Reset is initiated by the operator.

During the audit (Ref. 5), the NRC staff reviewed documents associated with the scram loop and its relays. The vendor successfully tested these components to demonstrate their proper installation and operation.

Based on the information provided, the NRC staff finds that the RPS is always capable of completing protective actions by shutting down the reactor once a scram is initiated. Further, the scram loop is designed to maintain reactor shutdown without operator action. Accordingly, the NRC staff concludes that the scram meets the design acceptance criteria for completion of protective action identified in NUREG-1537, Part 2 and Section 5.7 of ANSI/ANS-15.15-1978 and is acceptable.

(k) Surveillance

The guidance in Section 7.4 of NUREG-1537, Part 2 recommends that the system can be readily tested and maintained in the designed operating condition. ANSI/ANS-15.15-1978 recommends the system design include capability for periodic checks, tests, and calibrations. Additionally, if online periodic testing is necessary, such testing should not reduce the capability of the system to perform its safety function.

As described in Sections 3.2, 3.3, and 3.7 of this SE, the proposed I&C system includes the necessary features, including display of any necessary parameters or alarms to the operator, to facilitate the performance of the required surveillance checks, calibrations, and inspections required by the TSs and these design features provide acceptable provisions to demonstrate operability of the I&C system.

During the audit (Ref. 5), the NRC staff went to the control room to see the proposed control console, which includes the computers (User Interface Terminal and Console Computer System), display monitors, control panels, modularized drawers, indicators, meters and recorders, and printer.

Section 50.36(c)(3) of 10 CFR requires the surveillance requirements relating to test, calibration, or inspection to assure that the necessary quality of systems and components is maintained, that facility operation will be within safety limits, and that the limiting conditions for operation will be met. In addition, the design acceptance criteria for the RPS in Section 7.4 of NUREG-1537, Part 2 recommends that the RPS be sufficiently distinct in function from the RCS that its unique safety features can be readily tested and verified.

In Section 7.1.1 of the proposed SAR, the licensee stated that regular functionality tests, operations, and calibrations are sufficient to alert facility staff of deteriorating system performance. The licensee identified the surveillance requirements and periodicities in AFRRI TS Section 4.

TS 3.2.1 (c) requires that the scram time of the reactor be less than one second, and TS 4.2.1 (b) requires that the time to drop for all control rod rods be measured

semiannually, not to exceed 7.5 months. Also, this time should be tested after work is performed on any rod or its rod drive mechanisms.

TS 3.2.2 identifies the systems required to safely operate the reactor. Section 4.2.2 identifies the proposed surveillance requirements to verify the performance and operability of the systems and components that are directly related to reactor safety. These systems are neutron flux channel, fuel temperature channel, emergency stop scram, low pool water scram, and console manual scram button. In the LAR, the licensee stated that the current surveillances were not modified in the LAR, with the exception of the High Voltage Loss to Safety Channel. This safety channel did not include a surveillance in the TS. In LAR Rev. 1, Section 3.1.4 (Ref. 4), the licensee revised its TS to add this surveillance requirement for NP-1000 and NPP-100 safety channels to Section 4.2.2.c of the technical specifications. This modification to the TSs is evaluated in Section 3.11 of this SE.

The CCS and UIT include watchdog timers to ensure reliable communication and operation of these computers. The watchdog timers can be tested manually (with the rotary switch) or by software during the prestart tests. On the Reactor Control Mode Panel there is a rotary selection dial "SCRAM AND INTERLOCK TEST 2" that can be used to manually test the UIT and CCS Watchdog. Using the computer, testing is done by instructing the computer to stop sending refresh signals and then counting off the seconds and making sure a watchdog timeout occurs after some time period (e.g., 10 seconds). During the audit (Ref. 5), the NRC staff observed the rotary switch that the operator uses to test them.

Section 3.2.4 of the SAR indicates that the reactor control mode control pane includes two rotary test switches for the scrams and interlocks. These switches provided their signal to the CSC causing the CSC to perform the required functions. Section 3.2.4.3 of the LAR describes these rotary switches. During the audit, AFRRRI staff described how the scram and interlock test rotary switches on the reactor mode control panel. They demonstrated rotary test switch operation by placing each rotary switch in the period test position. The NRC staff observed appropriate indication in the control panel. AFRRRI also explained that both rotary switches can be used to run two different tests simultaneously.

The RPS includes a pulse time scram signal to ensure that the reactor power level will return to a low level after pulsing. The scram will be generated by the software logic in the CSC to scram all rods. So, when the defined time is reached, the software will send a signal to de-energize the associated relay in the scram loop.

Based on this information, the NRC staff finds that the system can be readily tested and maintained in the designed operating condition. The NRC staff also finds that the system design include capability for periodic checks, tests, and calibrations. Additionally, if on-line periodic testing is necessary, such testing does not reduce the capability of the system to perform its safety function.

(I) Classification and Identification

During the audit, AFRRRI staff showed the DAC cabinet and its drawers, components, and connections. Also, AFRRRI staff showed the wiring diagrams for the DAC and their connections to other I&C systems. The NRC staff observed that the wires were color

coded to identify the safety (white and red strips) and non-safety (white) signals, as well as the labels to identify each relay in the scram loop.

Also, during the audit, AFRRRI staff showed the wiring for the rod control system and the rod drive assembly, installed on the reactor bridge. AFRRRI staff explained that all cables from the DAC to the connecting rod assembly were replaced, but wires from the assembly to the control rod drive were not replaced. The NRC staff observed the new wires, and noticed that cables were not labeled, and the connections included cables that were no longer in use. AFRRRI staff explained that the wire diagrams clearly label these cables, and the operator could use the wiring diagrams to distinguish between them.

Based on the LAR descriptions and observation of the RPS, the NRC staff finds that the proposed I&C system identify the safety signals associated with the scram loop for a trained operator to distinguish between safety and non-safety systems and components. However, the cables associated with the rods are not labeled in the field but identified in the wiring diagrams. Although the rod's wires are not labeled, the NRC staff finds that the proposed RPS meets the design acceptance criteria for classification and identification in Chapter 7 of NUREG-1537, Part 2 and Section 5.11 of ANSI/ANS-15.15-1978.

(m) Environmental Qualification

Section 3.1 of this SE identifies AFRRRI's atmospheric conditions for the proposed I&C system. In Section 7.1.1 of the proposed SAR, the licensee stated that other than aging, there are no environmental conditions which have the potential for a functional degradation of the Reactor I&C system. In Sections 3.1.1 and 7.1.1 of the proposed SAR and LAR (Ref. 4), the licensee stated that the system did not undergo electromagnetic frequency interference/radio frequency interference (EMI/RFI) tests, however, best design practices were used to separate digital from analog signals to minimize the potential for interference. Also, instruments were constructed with metal enclosures to minimize outside interference and incorporate AC input to filters to suppress conducted noise.

The NRC staff evaluated the environmental conditions where the I&C system is installed and compared them to the manufacturer data for this equipment. The data shows that the proposed I&C system can operate in the AFRRRI conditions and concluded the I&C system is designed for reliable operation for the conditions anticipated within the facility. The environmental conditions in the reactor and control rooms are maintained by the HVAC system. The licensee also indicated that there are no credible physical or electrical interference scenarios where experimental or other components would interfere with reactor systems.

Based on the information provided and reviewed, the NRC staff finds the proposed I&C system is qualified for the intended operating environment and was designed such that in abnormal conditions, the reactor will fail-safe (i.e., scram) and that the proposed I&C system meets the design acceptance criteria for equipment qualification in Section 7.4 of NUREG-1537, Part 2.

(n) Human Factors

Section 3.7 of this SE describes the control console and displays to operate the AFRR1 TRIGA Reactor. This section includes the staff description and evaluation of the principles of human factors used in the proposed I&C system. In Section 7.6.4 of the proposed SAR (Ref. 4), the licensee stated that information in the human machine interface (HMI) was designed such that a minimal number of “clicks” are necessary for display navigation. Also, important manual control inputs such as rod pushbuttons and switches are given an independent physical panel through which they can be activated.

The licensee required that the reactor operator should be able to view critical reactor parameters at all times and that the operator should be able to find historic information of a facility parameter (as well as its current value). This information will allow the operator to view parameters on the main display of the control console. During the audit, the licensee demonstrated several functions on the control console with the proposed I&C systems.

The left side panel of the control console includes the STATUS pane, WARNING pane, and SCRAM pane to display information of which the operator should be aware. Section 3.7.3.1 of this SE describes these panes. In addition, the control console includes information for normal reactor operation, such as graphic scales indicating power, a graphic scale to indicate period, graphic scales to indicate fuel temperature, a graphical representation of the reactor cross section with information about the status of the control rods, and indication of the core position in the reactor pool.

In addition, the control console includes an emergency stop switch for the operator to stop door motion and core motion. The emergency stop switch and/or emergency stops will initiate a reactor scram and give scram indication to the operator on the console. Also, the magnet power key switch will scram the reactor if the key is moved to the OFF position. During the audit, the NRC staff reviewed the magnet power circuitry and confirmed that signals from the control console key switch and manual scram buttons will interrupt power to the magnet circuitry, causing the reactor to scram. The NRC staff reviewed the logic for operation of the key switch and manual scram buttons, labeling, and location. The NRC staff also reviewed the tests results from their acceptance tests, FAT, and SAT that tested configuration and operation of the key switch and manual scram buttons to scram the reactor. The NRC staff confirmed that the operators will have ready access to the key switch and manual scram buttons and that these will perform their safety function.

In addition to the variables monitored and controlled to safely operate the TRIGA reactor, there are process instruments necessary for the operation, such as pool temperature. These variables have continuous indication on the control console and are monitored and recorded. If the operator observes that these parameters are outside their range of operation, the operator can start a controlled shutdown of the reactor via the operator console or via the manual scram buttons.

Based on its review of the information provided in this section, the NRC staff finds that the proposed RPS includes readily available indication of AFRR1 TRIGA parameters and safety variables. The NRC staff's audit observations confirmed that the indications and locations of these parameters were designed in accordance with AFRR1's principles for the operator to have continuous view of important reactor parameters and access to

historic information of a facility parameter with ease and minimal operator actions. Accordingly, the NRC staff concludes that the proposed RPS meets the acceptance design criteria for human factors identified in NUREG-1537, Part 2.

(o) Prioritization of Functions

The magnet circuitry for AFRRI consists of relays in series, receiving scram signals from the neutron channels, fuel temperature monitors, manual scrams, CSC, and the magnet key switch. Therefore, any signal received from these systems to interrupt power to the magnet circuitry, or loss of power itself, will independently scram the reactor.

The CSC includes signals in the scram loop to shut down the reactor. However, the CSC does not have any priority over safety actuation devices.

During the audit, the NRC staff reviewed the logic in the CSC to confirm that it does not affect the independent operation of the scram loop. The NRC staff finds that, even if all parameters from the neutron and fuel temperature monitors are unavailable to the operator in the control console, the values of these indications are still accessible on the front panel of these channels.

Based on the information provided and reviewed, the NRC staff finds that the scram loop will independently initiate a reactor scram and the CSC will not undermine this capability. The NRC staff concludes that the proposed scram loop meets the design acceptance criteria of the NUREG-1537, Part 2 for the scram loop to prioritize signals from safety and non-safety sources.

(p) Quality

Table 8 of the LAR Supplement 1 (Ref. 4) identifies the contacts used for the scram loop. The licensee replaced the scram loop's components, such as wiring and relays with COTS components. In the SAR and LAR, the licensee stated that they performed rigorous testing and quality assurance at multiple steps in the scram loop design, manufacture, and installation process. During the audit (Ref. 5), the NRC staff reviewed test documents for the scram loop, including the acceptance test, FAT, and SAT. In addition, the NRC staff reviewed quality documents and procedures utilized by the vendor of these components. Section 3.10 of this SE provides the NRC staff's review of the quality process, development, and testing for the scram loop.

Based on its review of the information provided above and the discussion in Section 3.10 of this SE, the NRC staff concludes the scram loop was developed in accordance with the vendor's QA plan and procedures and properly documented and certified by the licensee. The NRC staff also finds that the licensee followed the ANSI/ANS-15.8-1995 guidance to identify, follow, and document applicable design inputs, such as design bases, performance requirements, regulatory requirements, codes, and standards. The NRC staff concludes the design of scram loop meets this criterion and is acceptable.

The NRC staff evaluated the RPS design in accordance with the design acceptance criteria identified in Section 7.4 of NUREG-1537, Part 2. Based on the evaluation of the information presented above, the NRC staff concludes as follows:

- The design criteria followed produced a reliable, capable, and suitable RPS for operation and protection of the AFRRRI TRIGA reactor. The protection channels and protective responses are sufficient to help ensure that the SL, LSSS, and RPS-related LCOs discussed and analyzed in the SAR will not be exceeded.
- The design reasonably ensures that the design bases can be achieved, the system will be built of high-quality components using accepted engineering and industrial practices, and the system can be readily tested and maintained in the designed operating condition.
- The RPS design is sufficient to provide for all isolation and independence from other reactor subsystems required by SAR analyses to avoid malfunctions or failures caused by the other systems.
- The RPS is designed to maintain function or to achieve safe reactor shutdown in the event of a single random malfunction within the system.
- The RPS is designed to prevent or mitigate hazards to the reactor or escape of radiation, so that the full range of nominal operations poses no undo risk to the health and safety of the public, the facility staff, or the environment.

3.7. Control System Console and Display Instruments

Section 7.6 of the proposed SAR, Section 6 of the LAR (Ref. 4), and Section 2.2 of the FRS (Ref. 15) describe control console and display instruments. The operators use the CSC to safely startup, modify reactor parameters, monitor operating parameters, and safely shutdown the reactor.

The CSC includes the UIT and CCS computers, digital I/O drawer, rod control panel, reactor mode control panel, bar graphs, recorders, and power supplies and UPS. Section 3 of the LAR describes and compares the old configuration and equipment with the proposed replacement. The proposed CSC and displays are located where the old equipment was.

The UIT and CCS computers include displays, control panels, modularized drawers, indicators, meters and recorders to present data and controls for operation of the reactor. Further, operators can use the control console for testing the functionality of the system and performing startup testing. Figure 6-1 in the LAR and Figure 7-20 in the proposed SAR (Ref. 4) illustrate the proposed CSC block diagram.

The rod control panel includes reactor key switch and pushbutton switches necessary to control the movement of the control rod drive mechanisms. The reactor mode control panel includes pushbuttons and switches to apply instrument power, select operating mode, and select the power level for automatic mode.

The CSC receives power 120 VAC primary side power from the DAC AC power distribution system, which originates from the console UPS, as described in Section 3.2 of this SE. The CSC includes the digital Input/Output (DIO) drawer to isolate all digital inputs and outputs.

The following sections describe CSC components in more detail.

3.7.1. Console Computer System

Section 7.6 of the proposed SAR and Sections 3 and 3.3 of the LAR Supplement, Rev. 1 (Ref. 4) describe the CCS. The CCS computer runs Linux operating system (SUSE) for input and output operations, and handles input and output data, monitors the pushbuttons on the control rod panel and drives the indicator lights on the console. This computer was programmed using High Level Assembly (HLA¹) language, C++, and TRIGA Basic². TRIGA basic, used for programming the operation of the reactor, includes the software that interacts with the COTS I/O boards. The vendor left the TRIGA basic installed in the computer for AFRRRI to make changes and tests, as necessary. The licensee stated in Ref. 4 that the TRIGA basic is a development environment that includes all software necessary to program the CSC to operate the TRIGA reactor. AFRRRI staff will administratively control access to the TRIGA program. Further, the licensee's staff noted that operators cannot change anything that impacts the safety of the system because the reactor trips are all analog and can only be changed at the respective NI modules located outside the control room.

The CCS gathers data from the DAC and process I/O signals to perform its function. The CCS uses a custom General Atomics (GA) protocol for communications to the rest of the system. The software to modify the communication protocol is part of the TRIGA basic.

The CCS includes a display that is used for startup and shutdown of the CCS and debugging the console software. The operator can also use the UIT to shut down the CCS. This display is not required during operation of the reactor; and if it is turned on, it will show the data from DIOs being constantly refreshed. If the data is not updated, this will indicate that the system is frozen.

In the LAR, the licensee proposed replacing the following devices, switches, or pushbuttons to be performed entirely in the CCS software:

- Pulse timer and steady-state scram timer functions
- Count-down/count-up scram timer
- Maximum pulse
- Rod bank selections

The licensee stated that the functionality and operation were not modified. The licensee also stated that all other physical switches will maintain their current functionality and remain unchanged. Consequently, the operator will use the physical switches to make selections, and these selections are read by the computer as a digital input and enforced by software. Section

¹ HLA is a public domain /open-source embedded programming language.

² TRIGA BASIC is an extension of the public-domain open-source HLA Basic language.

2.3.7 of the FRS (Ref. 15) describes software functions that will be provided to allow banked automatic movement of Reg only, Shim/Reg, Safety/Reg, and Shim/Safety/Reg. In Section 7.6.2 of the proposed SAR, the licensee explained that operators can use the CCS to perform the startup test. Using the startup test mode, the operator can cycle through the required checks prior to starting operation (i.e., prestart tests). Section 3.7.3 of this SE describes the display and operation of the prestart tests from the control console. The control console includes an administrative mode to allow approved facility personnel to perform more advanced testing of the system. During the audit, the NRC staff observed the display for the startup test mode.

The CCS and UIT include a watchdog timer to monitor operation of the computers. The watchdog timer is part of the scram loop. If the watchdog timer fails to send a signal every 7 seconds, the reactor will scram.

The CCS receives signals from systems to implement the following interlocks:

- The NLW-1000 sends a 1-kW permissive interlock. This signal is used to prevent using the pulse mode when power is above 1 kW.
- Interlocks necessary for each reactor operation mode, as described in Section 3.4.3 and summarized below.
 - Pulse mode – interlock to prevent the Shim, Safe, and Reg rods from being withdrawn.
 - Steady state mode – interlock to ensure that only one control rod can be manually withdrawn at a time in the manual mode.
 - Steady-state – interlock to prevent the application of air to the transient rod drive mechanism unless the drive cylinder is fully inserted (all the way down with the rod down limit switch active).
 - Square Wave mode – interlock to ensure that only one control rod can be manually withdrawn at a time, excluding the Transient rod. (Note that after firing the Transient rod, the system moves from SQUARE WAVE to AUTO mode, and the Transient rod is then treated like any other rod and cannot be moved by the operator.)
- RWP interlocks to prevent any positive reactivity from being inserted into the core until specific conditions are satisfied. These conditions and interlocks are described in Section 3.4.4 of this SE.

Logic for operation of the AIR, UP and DOWN buttons is performed in the CSC. Section 3.4.1 of this SE describes the operation of these buttons to move the rods.

The control console includes the logic for the different operating mode of the reactor. The graphics display includes four software-based pushbutton mode selector switches. Section 3.4.3 of this SE describes reactor modes.

3.7.2. User Interface Terminal Computer

The UIT runs Windows 7 operating system. This computer includes its own monitor to display parameters and accept user input. The UIT code was written in HLA BASIC. The UIT is used as a display driver for GUI.

In addition, the licensee proposed upgrades to the system data logging and historian. These upgrades consisted of only starting up and running the History Playback module after shutting down the reactor operating software. Section 2.3.11 of the FRS (Ref. 15), Section 3.4.4.2.7 of the LAR Supplement Rev. 1, and Section 7.6.4.2.2 of the proposed LAR (Ref. 4) describe operation of this module. The UIT computer records a log of events and device states on the hard disk using a date and time stamp. The computer begins recording after the reactor is reset. Data will be recorded approximately every 100 milliseconds until it is terminated by the operator, even after a reactor scram. The UIT will record any event or indication in the WARNINGS pane or the SCRAM pane. The system also records while the reactor is in a scrammed condition, creating a new data file every two hours. Further, the system logs each time an operator uses the console and the reactor megawatt hours.

The UIT uses a coded name (date and time) to identify each reactor run for easy searching. At the beginning of each new file, the input states are recorded from the end of the previous file to create continuity of the information between files. Logged data can be transferred to authorized removable media (e.g., memory stick drive) in accordance with AFRRI procedures.

The UIT computer includes the History Play back module to retrieve and view logged data. This module is separate from the UIT program. The reactor administrator or operator can use this module to retrieve logged data, or any particular reactor run, when the reactor is shutdown. If the reactor is running the history playback module won't work. The playback program does not affect any I/O on the system. The recorded log will show the control rod movements and bargraph displays at the time of operation. The operator can either manually or automatically play back the recorded data. For manual display, the operator can navigate through each recorded frame on the playback display. For automatic display, the data will be shown automatically in sequence at a variable speed.

In the LAR, the licensee also proposed replacing meters and readouts for variable indications in the control console graphical displays, as well as upgrading the old bargraphs and recorders. Sections 3.7.8 and 3.7.9 of this SE describe the proposed bargraphs and recorders.

3.7.3. Control Console Displays

Section 6 of the LAR, Section 7.6.3 of the proposed SAR (Ref. 4), and Section 2.3.2 of the FRS (Ref. 15) describe the control console and displays. The control console includes two high-resolution display screens. The displays monitor the following parameters:

- Reactor wide-range linear power from NMP-1000
- Reactor wide-range log power and period from NLW-1000
- Reactor linear power from NP-1000
- Reactor linear power from NPP-1000
- Reactor fuel temperatures

- Reactor pool temperature
- Rod position
- Pulse data
- Information to test the reactor and computer I/O
- Prestart tests

This information has been grouped by type into two status displays to streamline information flow from the system to the operator. The Left-Side STATUS display shows information about the operation and status of the reactor, such as scram status and any operational warnings or interlocks, using text. The Right-Side GRAPHIC display shows reactor operations and status in graphical format. The following subsections describe these panels in detail.

The control console includes a keyboard and a mouse for the operator to enter data and/or navigate the displays. The console also includes a printer for operators to print the results of the prestart checklist, operator histories, etc. The printer is located inside the cabinet housing the control console. During the audit, the NRC staff observed the location of the printer inside the locked cabinet.

3.7.3.1. Left-Side Status Display

Section 7.6.4.2.1 of the proposed SAR and Section 6.3.1 of the LAR (Ref. 4) describe this display. This display includes five panes: Status, Scram, Warnings, Mode Selection, and Interlocks. These panes are simultaneously visible in the display. During the audit, the NRC staff observed this display and its panes.

a) Status Pane

This pane shows the current status of the reactor, including power level, period, pool temperature, outlet and inlet temperatures, low pool level status, core position, and shielding door positions.

This pane also shows the remote/local state of each channel to indicate if the channel has been placed in remote (front panel enabled) or remote CSC control. During a pulsing operation (Ref. 16), an additional inhibited field will be shown for the NLW and NMP and an additional bypassed field will be shown for the NP. These fields are displayed to the right of the remote/local field. In Ref. 16, the licensee explained that these are generated by the control console (software), which would transmit a bypass signal to the NP-1000 and inhibit signals to NLW and NMP to disconnect their electrometer during pulse. The system will automatically remove these signals after the pulse is completed and the reactor is scrammed.

b) Scram Pane

This pane shows the events or conditions that generated a scram. This pane will show the system scram signal in a red box when generated.

NOTE: All scram/alarm messages displayed on the SCRAM and WARNINGS panes are first displayed on the left STATUS display, as opposed to the information panes on the graphic display.

c) Warnings Pane

This pane shows a yellow box and audible alarm for identifying warnings for the operator to be aware of an event. This pane will show warnings from: NMP-1000, NP-1000, NPP-1000, NFTs. The caption of the warning will appear when the condition is detected. This pane has a checkbox for disabling each alarm. If the checkbox is checked and a trip occurs, the yellow box will continue to be displayed to warn the operator, but there will be not sound from the horn.

d) Mode Selection Pane

This pane allows the operator to select the mode of operation. Section 3.4.3 of this SE describes the reactor modes of operation.

This pane also includes objects for the following commands:

- Setting for demand power – the operator can use the text box and the set demand button to enter a desired power level (in watts) when the reactor is operating in Automatic mode. Once the level is selected and the button is pressed, the control system will move the rods selected in the banked movement to insert or remove reactivity to maintain power at the demand setting.
- Selection of NMP-1000 Range – During normal operations, the NMP-1000 automatically change its scale based on the reactor power. The operator can use the text boxes with checkboxes to manually select the NMP-1000 Range, which can be done during any mode of operation. The values available are Auto range, 1 MWt, 100 kWt, 10 kWt, 1 kWt, 100 Wt, 10 Wt, 1 Wt, 100 mWt, and 10 mWt. If the power continues to rise and the NMP-1000 reaches 110% of its selected scale, it will initiate a scram, providing diversity for safely operate the reactor.
- Setting for timed actuations – the operator can select the length of time for the pulse time and scram time. To set either time, the value is entered in the text box and then actuated by pressing the Set Time button in the display. The operator can also use buttons provided to start, stop, and reset, count up, and count down the timer. During pulse mode, the operator manually scram the reactor after a few seconds. But the system will scram the reactor when the Set Pulse Time limit is reached, as required by TSs. The maximum time for this timer is 15 seconds. During steady-state (or manual) mode, the operator uses the Set Scram Time to define the running time and then scram the reactor.

e) Interlocks Pane

This pane shows interlocks that are active by displaying a yellow box for that interlock. This pane has a checkbox for disabling each notification in the Annunciator Pane. If the checkbox is checked and an interlock occurs, the yellow box will continue to be displayed in the Annunciator Pane to notify the operator, but there will be not sound from the horn.

3.7.3.2. Right-Side Status Display

Section 7.6.4.2.2 of the proposed SAR and Section 6.3.2 of the LAR (Ref. 4) describe this display, which the operator uses to monitor and control the reactor. The display always shows the system menu bar, display menu bar, system status box, and annunciator box.

At the top right corner, the display always shows the system menu bar, which includes the following menu items:

- RUN: Exit to Windows or restart the UIT.
- OPERATOR: Provides the ability to log in, log out, and display selected operator statistics.
- HISTORY: System must be scrammed, then starts the execution of the history playback program.
- DISPLAY: Refreshes the graphics displays (this option is rarely used).

At the left top corner, the display always shows the system status bar, which includes the following items:

- Date and time
- Mode
- Reboot time
- Demand power

In the upper middle section, the display shows the annunciator box. This section will only appear in the screen to identify interlock, warning and/or scram messages when they occur. The size of this box will change to accommodate the number of messages received. Scram messages have higher priority and therefore, they would be presented at the top of the message box. The operator would use the Acknowledge button on the Rod Control Panel to recognize the message. Once a message is acknowledged, it would disappear from the box.

This display consists of the following screens:

- Reactor Display #1

This display consists of bargraphs to show status of monitored variables (e.g., current reactor power), the rod drop times for each rod, a graphical representation of the reactor with the position of the rods, status of the rod control buttons in the Rod Control Panel, and a graphic representation of the reactor position, shield door position, ER door 1 and door 2 positions.

- Reactor Display #2

This display can be configured by the operator, under administrative controls. The factory configuration is similar to Display #1, with the exception of not including a graphical representation of the reactor with the position of the rods. Instead, this configuration includes a strip-chart recorder to display four selected variables.

- Reactor Prestart Tests

This display is only available when the reactor is scrammed and magnet power is not applied. This display will show the prestart tests available that are programmed in the CSC. When each test is completed, the display will show either Pass or Fail, along with

the reason. At the end of the test, the operator will press on the Done button to clear all prestart tests and return to Display #1.

- Pulse Display

This display will automatically be shown after a pulse operation to show results from the pulse operation. The operator can also view this display if the reactor is scrammed to see results from previous pulse operation.

- Administration

This display is only available when a system administrator is logged in. The display will show operator statistics (e.g., operator running time, reactor power, etc.)

- Test Functions (for system administrator use only)

During reactor operation, Reactor Display #1 and Reactor Display #2 are shown on the top display, in the form of tabs, to show reactor operation and status. During the audit, the NRC staff observed this display and its screens.

3.7.4. Digital Input Drawer

Section 3 of the LAR describes the proposed digital input drawer. This drawer includes digital input boards and isolators to isolate all digital inputs and outputs located in the control system console and send them to the Control System Computer.

3.7.5. Utility Drawer

Section 7.6.3.5 of the proposed SAR and Section 6.3.10 of the LAR (Ref. 4) describes the proposed Utility drawer. This drawer contains the CCS and UIT watchdog timers, I/O module, and digital outputs.

3.7.6. Rod Control Panel

Section 6.3.4 of the LAR, Section 3.1 of LAR Supplement, and Section 7.6.3.6 of the proposed SAR (Ref. 4), and Section 2.3.5 of the FRS (Ref. 15) describe the rod control panel. This panel manually controls the control rod drives, applies magnet power, fires the transient rod, manually scrams the system, and acknowledges messages in the Annunciator Pane of the control console. Figure 35 in the LAR Supplement Rev. 1 (Ref. 4) shows an illustration of the proposed panel. The CSC displays the position of the control rod. The display also shows the status of the control rods, which are only graphical representation of the buttons on the Rod Control Panel. These display objects cannot perform any actions.

To manually control the CRD, the operator uses the following pushbuttons:

- UP or DOWN pushbuttons for moving the transient, shim, safety, or regulating rods.
- MAGNET pushbuttons for turning off magnet power the shim, safety, or regulating rods. This action will drop the rod into the reactor core.

- FIRE pushbutton for applying air pressure to the transient rod for pulse mode, if required conditions are met.
- AIR pushbutton for removing air from the transient rod.

The proposed Rod Control Panel does not directly control the control rods. When the buttons are pressed, a signal is transmitted to the CCS computer which in turn provides the control logic for the control rods. Pressing the UP or DOWN pushbuttons generates a digital input to the CCS computer to move the control rods. Section 2.3.24.1 of the FRS (Ref. 15) and Section 7.3.3.1 of the proposed SAR (Ref. 4) describe the operation of these pushbuttons. Only one UP pushbutton may be pressed at a time. If multiple UP pushbuttons are depressed, the system will not activate. The system does not activate control rod movement upon an UP and DOWN pushbutton command for the same rod. Any number of DOWN pushbuttons may be pressed simultaneously. To power the magnet circuitry, the operator uses the Magnet Power key switch. The switch has three positions: OFF, ON, and RESET. The ON and OFF positions are maintained by a permanent contact. The ON position is part of the scram loop, and it is required to power the magnet circuitry and supply air to the transient rod. The OFF position will remove power from the rod magnets and air supply to the transient rod. To move the switch from the OFF position to ON, the switch passes through the RESET position. The RESET position uses a momentary contact. It generates a digital input to the software that is only present as long as it is activated by the operator. The RESET is used for resetting the scram loop via the KEY RESET relay and start the time delay in the FIS prior to activating the reactor permissive relay (ROX). The reactor will be scrammed by turning the magnet power key switch to the OFF or RESET positions. During the audit, AFRRI staff demonstrated operation of the magnet power key switch. After a scram, to restart the reactor, the operator needs to move the Magnet Power key switch to the RESET position and follow the steps described before.

To fire the transient rod when in pulse mode, the operator uses the FIRE button in the control panel. Pressing this button will apply air pressure to the transient rod for pulsed reactor operation. Section 3.4.3 of this SE describes pulse mode.

To acknowledge signals, the operator uses the ACKNOWLEDGE button in the Rod Control Panel. The ACKNOWLEDGE pushbutton will acknowledge any scrams, warnings, or interlocks shown on the annunciator pane of control panel.

This panel includes the SCRAM button for the operator to shut down the reactor. The signal from this pushbutton is directly linked to the scram loop, and it is not processed in the CSC. Pressing this button will interrupt power to the magnet circuitry. This signal is also transmitted to the control console for indication.

3.7.7. Reactor Mode Control Panel

Section 6.3 of the LAR, Section 3.2 of the LAR Supplement Rev. 1, Section 7.6.3.7 of the proposed SAR (Ref. 4), and Section 2.3.5 of the FRS (Ref. 15) describe the rod control panel. The operator uses this panel to control the reactor mode, test functions, and for indication of the reactor status. This panel also includes the pushbutton to power instruments for the control systems and an emergency stop pushbutton. When pressed, switches and pushbuttons, with the exception of the emergency stop pushbutton, transmit a signal to the CSC to perform the logic.

The panel is divided in the following sections:

- Core position – this section of the panel provides information of the reactor core. It includes switches Region 1 and Region 3, an indicator for Region 2, and a digital readout. The operator uses the Region 1 or Region 3 switches to move the reactor core to that position. The operator can also use the foot pedals to move the reactor. These switches will illuminate when the door limit switch is activated. The indicator for Region 2 will illuminate when the core is not in Region 1 or Region 3.
- Door position – this section includes switches and indicators for the lead door open, lead door close, and lead door stop. The operator uses these switches to operate the lead door. The switch will illuminate when the signal is active. An indication is also provided in the control console.
- Indicators – this part of the panel includes indication for operation of the Reactor, Time Delay and Exposure Room Open. The Reactor Operate indicator is illuminated when all interlocks have been satisfied and magnet power can be applied. The Time Delay indicator is illuminated while the 30-second reactor interlock delay is active. The Exposure Room Open is used to indicate that the ER door is open.
- Push buttons – the control panel includes: the lamp test button to test the lamps and indicators in the panel, the pulse detector button to select the detector connected to the NPP-1000 for steady-state mode or for pulse mode, and an emergency stop (latching) switch to scram the reactor in an emergency. The signal from the emergency button is connected to the FIS. Pressing the button once, deactivates the reactor permissive relay that is an input to the scram loop. These buttons are latching but push to activate and twist to deactivate.
- Control system – this section includes the Instrument Power ON button to power the UPS and instruments. Pressing the pushbutton once will activate the UPS. If pressed again, then power to the UPS will be removed. This button will illuminate when the console power is on.
- Watchdog timers – this section includes two indicators that will illuminate to indicate if the watchdog timer for CCS or UIT timeout has occurred.
- Scram and interlock test rotary switches 1 and 2 – this part of the panel allows the operator to test scrams and interlocks. Because of the number of signals, they are separate in rotary switch test 1 and rotary switch test 2. The operator uses the rotary switch to select the test to be performed. Once the selection is made, the operator pushes the test button associated with the rotary switch to run the test. The operator can simultaneously activate both rotary switches to perform multiple tests.

Rotary switch test 1:

- >1 kW – to test the 1kW interlock
- Source – to test the NLW low source interlock
- Period – to test the NLW period low interlock
- NLW HV Lo – to test the NLW low high voltage interlock
- NMP HV Lo – to test the NMP low high voltage interlock
- NMP Power Hi – to test the NMP high-power scram

- NP HV Lo – to test the NMP low high voltage scram
- NP Power Hi – to test the NP high-power scram
- NPP HV Lo– to test the NPP high-power scram
- NPP Power – to test the NPP high-power scram

Rotary switch test 2:

- FT 1 – to test the high temperature scram
- FT 2 – to test the high temperature scram
- FT 3 – to test the high temperature scram
- Pool Temp – to test the reactor pool water high temperature interlock to prevent rod withdrawal interlock
- Pool Lo – to test the reactor pool low level scram
- CCS Watchdog
- UIT Watchdog

3.7.8. Bargraphs

Section 6.3.5 of the LAR, Section 3.5 of the LAR Supplement Rev. 1, and Section 7.6.3.5 of the proposed SAR (Ref. 4) describe the proposed replacement for the bargraphs installed in the control console. They are microprocessor-based LED meters that receive analog 4 -20 mA signals from the reactor instruments to provide independent power and fuel temperature indications. The control console includes the following LED bargraphs:

Instrument	Variable	Range
NP-1000	Linear power level	0-120%
NPP-1000	Linear power level	0-120%
NLW-1000	Log power level	1 E-8 to 100% log power
NLW-1000	Period	-30 to 3 sec period
NFT-1000 channel 1	Fuel temperature	0-1000 °C
NFT-1000 channel 2	Fuel temperature	0-1000 °C
NFT-1000 channel 3	Fuel temperature	0-1000 °C
NPP-1000	NVT ³ - pulse	0-50 MW-sec
NPP-1000	NV ⁴ peak - pulse	0-6000 MWt

In Section 3.5.4 of the LAR Supplement Rev. 1 (Ref. 4), the licensee described an interlock between the NPP-1000 NV and the CCS. This interlock is used during pulse mode. The input to the NPP-1000 NV Peak is wired to one of the relays on the utility drawer in the CSC. The CCS controls this relay to be active only during pulsed reactor operation. During steady state operation, the input to the bargraph is disconnected because the NPP peak produces an output at all times but only needs to be displayed during pulses.

3.7.9. Recorders

³ The unit “nvt” represents time integrated flux n/cm²

⁴ The unit “nv” represents flux in n/cm²/sec

Section 6.3.5.2 of the LAR, Section 3.6.4 of the LAR Supplement Rev. 1, and Section 7.6.3.8.2 of the proposed SAR (Ref. 4) describe the proposed digital chart recorders to replace the old paper charts. The NP-1000, NPP-1000, NLW-1000 power channels and the NFT-1000 fuel measuring channels provide independent analog signals to the chart recorders. Table 10 in the LAR identifies all inputs connected that can be recorded. The operator can add additional inputs to the recorders, if necessary. As a minimum, the recorders were configured to provide the following indications:

- NLW-1000 log power
- NP-1000 linear power

3.7.10. Technical Evaluation of the Design Bases of the Control Console and Display Instruments

This section of the SE provides the NRC staff's evaluation of the design basis of the control console and display instruments against the acceptance criteria identified in the guidance of Section 3.1 and Section 7.6 of NUREG-1537, Part 2.

Section 50.34(a)(3)(ii) of 10 CFR requires the applicant to describe the design bases and the relation of the design bases to the principal design criteria, and 10 CFR 50.34(b) requires updating the information to take into account any pertinent information developed since the submittal of the preliminary SAR. Section 7.6.2 of the proposed SAR describes the design basis for the control console. In addition, in Sections 3.1.5 to 3.6.5 of the LAR Supplement Rev. 1, the licensee provided safety analyses for the proposed control console and display instruments. In addition, in Sections 3.1.3 to 3.6.3 of the LAR Supplement Rev. 1, the licensee provided comparisons of the previous system and the proposed new systems.

The previous console included a single computer, two displays, chart recorder, count-down/count-up scram timer, a maximum pulse timer, a History Playback software module, switches for the rod bank selections, a DC digital input/output, a rod control panel, a reactor mode control panel, bargraphs, recorders panel, and auxiliary console. These devices were used to monitor actions performed in the control rod and reactor model panels, to display reactor power, control rod position, and other operating parameters on the monitors, and to receive operator's input to perform certain actions.

The proposed control console provides the same functionality as the previous system, but the licensee moved some of the functions that used to be performed by analog devices to the new system in which those same functions are now implemented in software. Section 3 of the LAR Supplement Rev. 1 compares the previous and the proposed new system.

The reactor operator has two scram options from the control console: manual scram push button and magnet power key switch scram. These two scram options control functionality for engaging the rod magnetic current.

The NP-1000, NPP-1000, NLW-1000 power channels and the NFT-1000 fuel measuring channels provide, independently, both an analog signal and a digital signal to the control console. The analog signal is used for display by the bargraphs and chart recorder and by the console computer display interface. The reactor operator can use these independent signals to cross-check the validity of the indicated power level or fuel temperature. Therefore, in the case that a bargraph fails, or provides erroneous information, there are other redundant and diverse channels that the operator can use to verify power level or fuel temperature.

Colors for the indicator lights on the console show the operator the status of the reactor. Figure 64 of LAR Supplement Rev. 1 and Figures 7-28 and 7-29 of proposed SAR (Ref. 4) shows that all trip indicators in SCRAM Pane are red and warning indicators in Warning Pane are yellow. The indicators and controls necessary for startup and shutdown operations are logically grouped in front of the operator.

In addition to the control console, an auxiliary console is also present in the control room. This auxiliary console was not modified in the LAR. The auxiliary console includes paper chart recorders for the radiation monitors and continuous air monitors, and provides indication for pool temperature, pool level, exposure room temperatures, and ventilation dampers. These indicators receive independent signals from the field instruments to provide a redundant and diverse indication of the monitored variables.

Based on the NRC staff's review of the design bases information provided in the LAR, proposed SAR, and observations during the audit, the NRC staff finds that the proposed control console/display instruments are adequate to perform the necessary control and protection actuation and information management, storage, and display functions to help ensure continued safe operation of the reactor. Therefore, the NRC staff concludes the AFRRI proposed control console and instrumentation design meets the design bases acceptance criteria in Section 3.1 and Section 7.6 of NUREG-1537, Part 2.

3.7.11. Technical Evaluation of the Design Criteria

This section of the SE documents the NRC staff's review and evaluation of the proposed design of the control console and display instruments to perform their functions based on the appropriate design criteria to satisfy the 10 CFR 50.34(a)(3) and (b) requirements. The NRC staff's evaluation of the design of the proposed control console and display instruments is based on acceptance criteria in Section 7.6 of NUREG-1537, including acceptance criteria from the guidance and industry standards referenced by Section 7.6 of NUREG-1537, Part 2.

Sections 7.6.1 and 7.6.2 of the proposed SAR (Ref. 4) describes the design criteria and design basis for the for the proposed control console.

a) Independence

Section 3.6.3(c) of this SE indicates that a failure or malfunction in the control console/display instruments does not prevent the RPS from performing its safety function and does not prevent the reactor from performing a safe shutdown.

b) Fail-safe

Section 6.1 of the LAR Rev. 1 states that the CSC is designed to fail-safe such that any failure will result in the reactor entering into a safe shutdown.

c) Prioritization of functions

Section 6.1 of the LAR Rev. 1 states that there are no protective functions that rely on the control console.

d) Surveillance

Section 6.4 of the LAR Rev. 1 states that there are no specific surveillance tests with the CSC that have not been previously outlined in this LAR. Operators will be required to validate acceptable console performance when performing normal facility prestart testing.

e) Human Factors

Section 2.4 of the LAR Rev. 1 states that consideration of human factors and man-machine interfaces has been included in developing the design of the system. The operator controls have been designed so that operators can perform their tasks easily and correctly. The choice of controls used in the system provides a simple error proof system that will optimize the operator's performance under all conditions.

f) Annunciators

Section 2.4 of the LAR Rev. 1 states that human-machine interface principles employed are ready access to design parameters in as few navigation actions as possible, text with suitable size for ease of reading and color coordination of the text and annunciator bars to indicate actuation versus nominal status

g) Quality

Section 3.1.7 of the LAR Supplement Rev. 1 states that the FAT demonstrated that the replacement I&C console meets the requirements of the FRS (Ref. 15). Additionally, GA performed separate, in-depth tests of the components, the nuclear instruments, the control system console, and the system as a whole.

Based on the information presented above, the NRC staff concludes that the LAR, as supplemented, contains sufficient control console/display information. Specifically, the NRC staff concludes:

- All nuclear and process parameters important to safe and effective operation of the AFRRI reactor will be displayed at the control console. The display devices for these parameters are easily understood and readily observable by an operator at the control console. The control console design and operator interface are sufficient to promote safe reactor operation.
- The design of the output instruments and the controls in the control console provides appropriate features for checking operability, inserting test signals, performing calibrations, and verifying trip settings.
- The annunciator and alarm panels on the control console provide adequate indication of the status of the reactor and its systems to support operators in safe operation and shutdown of the reactor.
- The locking key switch on the control console reasonably ensures that the reactor facility will not be operated by unauthorized personnel.

3.8. Process Instrumentation

Section 7.7 of the proposed SAR and Section 1.8 of the LAR Supplement Rev. 1 (Ref. 4) describe the process instrumentation. In these documents, the licensee noted that the original sensors were not modified, and the modification consisted of converting the analog signals to digital so they can be displayed in the upgraded control console. The AFRRI reactor includes instrumentation to measure variables to safely operate and maintain the reactor at a safe level, including heat removal from the core, protection against high radiation levels, and maintenance of the quality of the fuel clad. The variables measured include: the primary coolant temperature, primary water conductivity and pool water level. The licensee proposed modifications to the control console to display pool water level and primary water temperature.

3.8.1. Primary Water Temperature

Section 7.7.1 of the proposed SAR states that primary water temperature is measured near the core and in the bulk coolant volume to ensure the highest temperature point is monitored.

In Section 7.7.3.1 of the proposed SAR and Section 1.8.1 of the LAR Supplement Rev. 1, the licensee noted that the water temperature is measured by a resistance-temperature sensing element (detector) (RTD) in a bridge circuit with signal conditioners. The RTDs have a range of 0 to 100°C. The water temperature is sent to the CSC to provide a readout on the reactor status display. The AFRRI TSs defines the inlet water temperature limit to be 60°C. In Section 1.8.1 of the LAR, the licensee noted that the temperature sensors were not replaced as part of the LAR.

If the inlet water temperature reaches or exceeds this limit, the CSC will activate an interlock in the rod withdrawal interlock to prevent the further addition of positive reactivity by locking out all control rod withdrawals.

3.8.2. Primary Coolant Conductivity

Section 7.7.2 of the proposed SAR states that conductivity of the coolant is measured in the pump room. In Section 7.7.2 of the proposed SAR, the licensee noted that the conductivity is measured in micromhos/cm, and conductivity should not exceed 5 micromhos/cm as required by AFRRI TS 3.3.b with typical measurements being in the 2-3 micromhos/cm range.

Section 7.7.3.2 of the proposed SAR and Section 2.3.19 of the FRS (Ref. 15) state that water conductivity is measured by the conductivity cells contain titanium electrodes in microprocessor-based circuitry. Readouts for the conductivity monitors are displayed locally.

3.8.3. Pool Water Level

Section 7.7.1 of the proposed SAR states that pool water level is measured to ensure adequate cooling capacity, as well as protecting facility personnel from high radiation levels. Section 7.7.3 states that the level of the reactor tank water is monitored by two independent switches mounted on a rod and actuated by a float. The level measurement will provide an early warning alert on low water level (first switch), and a scram when the water drops below the setpoint (second switch). If the water level reaches the first switch, the CSC will generate a signal to the rod withdrawal to prevent the withdrawal of the control rods.

Section 2.3.15 of the FRS (Ref. 15) states that during non-duty hours, the scram signal will activate an audible alarm and visual warning on the annunciator panel in hallway 3101 to inform the security guard that an unusual situation is present so that appropriate action may be taken.

In Section 7.7.2 of the proposed SAR, the licensee noted that a float mechanism is used so that it is set to give a high/low status at the calibrated level. The accuracy of this measurement is at least to the nearest 1/2" inch of water.

3.8.4. Technical Evaluation of the Design Bases of Pool Water Level

Section 7.7.2 of the proposed SAR describes the design bases for the AFRRRI process instrumentation.

The primary water temperature is monitored to ensure heat removal. Section 7.4.2 of the proposed SAR states that following shutdown, the fuel temperature will return to equilibrium with the bulk coolant. The rate of temperature decrease is dependent on the differential between the fuel and coolant temperatures. In Section 7.7.2, the licensee noted that coolant temperature can range from several degrees C to boiling, but the AFRRRI TSs define the temperature limit to be 60°C. If the inlet water temperature reaches or exceeds this limit, the rod withdrawal will activate an interlock to prevent the further addition of positive reactivity by locking out all control rod withdrawals. However, this interlock does not prevent control rod insertion or scram the reactor.

In Section 1.8.5 of the SAR Supplement Rev. 1, the licensee notes that the water conductivity is measured to ensure the pool integrity by identifying any activation or fission products or contamination of the water. If the TS limit is reached, an alarm will be generated to alert the operator.

AFRRRI measures and monitors the pool water level ensures cooling capacity and radiation protection at the pool top. In Section 7.4.2 of the proposed SAR, the licensee states that AFRRRI TSs require this level to be no less than 14 feet from the top of the core. In Section 7.4.2, the licensee noted that when the pool is completely full, the value is approximately 16 feet. The measurement is performed by a float in the reactor pool. Low Pool Level is set when the pool level float switch indicates that the pool level has fallen 6 inches below normal. The reactor pool water ensures adequate radiation shielding to the reactor bay as well as cooling capacity to the reactor. Actuation of the pool float switch is visible from the control room or through visual inspection. The coolant level is maintained regardless of the operating state of the reactor. During a postulated accident, the coolant level should remain constant. Additional coolant water is available within the facility to provide replacement for any decrease in normal operating levels.

The Status pane shows current temperatures and pool water level. From the Reactor Mode Control Panel, the operator can run scram tests associated with pool level Low and pool temperature.

Figure 7-1 in the proposed SAR shows the pool level and water temperature, plus the water coolant inlet and outlet temp wired to the DAC.

3.8.5. Technical Evaluation of the Design Criteria

Section 7.7.1 of the proposed SAR describes the design criteria for the AFRRRI process instrumentation.

To address the potential for single failure, the AFRRRI reactor includes two different points to measure primary water temperature: near the core and in the bulk coolant volume. The operator monitors water temperature from the reactor status display. The reactor does not include a scram signal associated with primary water temperature. However, the CSC will generate a signal to the rod withdrawal interlock to prevent further addition of positive reactivity. Therefore, if the temperature increases beyond 60°C, in accordance with AFRRRI TS 3.3.a, then the operator will manually shutdown the reactor.

Similarly, AFRRRI measures conductivity in two different points to address single failure. The TSs define a conductivity limit, that if reached will generate an alarm.

The water level in the pool includes two switches for monitoring and scram the reactor. The first switch will alert the operator on low level and prevent the withdrawal of the control rods. The second switch will shut down the reactor.

The licensee specified the range of operation and TS limits for the process instrumentation, as described in Sections 3.8.1 to 3.8.3 of this SE. Table 7-9 of the proposed SAR provides the setpoints and resulting actions for pool level and temperature to maintain to ensure adequate cooling capacity and protect facility personnel from high radiation levels; primary water temperature to remove heat from the core; and water conductivity to detect radioactive material or contamination of the pool water.

When any of the process instrumentation identified in AFRRRI TS 4.3 reaches or exceeds the TS limit, an alarm will notify the operator to take action, such as immediate shutdown of the reactor. Section 7.7.4 of the proposed SAR provides the TS action items if these instruments fail to alarm or shutdown the reactor. The licensee did not modify these TSs in the LAR.

Based on the information provided, the NRC staff concludes that the process instrumentation components were designed to sense parameters necessary for facility operation and to transmit this information to the control console for the operator to perform actions specified in the AFRRRI TSs.

3.9. Access Controls

3.9.1. Description of Access Controls

This section documents the NRC staff review to confirm that the access control features that were part of the I&C system equipment upgrade (hardware, software, firmware, and interfaces) are adequate to protect the AFRRRI reactor from unauthorized access.

Section 7.1 of the proposed SAR, Rev. 1 (Ref. 4), notes that the CSC consists of two computers, the UIT to display reactor activities, and the CCS to control the reactor and monitor I/Os. These computers have a login system to grant access to the operators and AFRRRI personnel. In addition, the control console includes the UPS, I/O drawers, utility drawer, rod control panel, reactor mode control panel, bargraphs, and record panel. Section 7.6 of the proposed SAR provides detailed description of the proposed modifications to the CSC, including its design criteria and design basis.

Section 1 of the LAR, Rev. 1 (Ref. 4) describes the modifications proposed and control to access the CRDM and DAC. The proposed CRDM is configured from the control console, which is password protected, and its hardware is installed in a locked cabinet. The DAC and its housed equipment are locked. Section 6 of the LAR, Rev. 1 states that access control to the computer system in the control console includes a login/password scheme, which is further described in Section 8, "Cyber-Security." AFRRRI relies on multiple layers for physical access to the reactor I&C system and control console. The control console and auxiliary panel are located in the control room. The DAC, FIS, MCC, rod controls, and radiation monitors are all located in the reactor room. Access to the control room and reactor room is controlled via a door with access controls. Unescorted access to the facility and any facility controls is limited to personnel verified and authorized by the licensee, using access cards.

To prevent unauthorized use of the reactor and control system, AFRRRI uses a login/password scheme. Access levels would include operator and system administrator. Further, to prevent operation of the reactor, the reactor console includes the magnet power key switch, which requires a key that is locked.

3.9.2. Technical Evaluation of Access Controls

This section of the SE details the NRC staff's evaluation of the design basis using the acceptance criteria guidance in Chapter 7 of NUREG-1537, Part 2, including acceptance criteria from the guidance and industry standards referenced by Chapter 7 of NUREG-1537, as listed in Section 2 of this SE.

Section 50.34(a)(3)(ii) of 10 CFR requires the applicant to describe the design bases and the relationship between the design bases and the principal design criteria. 10 CFR 50.34(b) requires updating the information to take into account any pertinent information developed since the submittal of the preliminary SAR.

In the SAR Rev. 1, AFRRRI does not specify a design criterion for access control of its I&C systems. Nevertheless, in the SAR for renewal, AFRRRI described that access to the entire AFRRRI complex is controlled and all personnel are required to enter and exit the facility through the front and back entrances. As part of the license renewal process, AFRRRI submitted a physical security plan for its reactor facility, which includes AFRRRI's procedures and security measures for the physical protection of the AFRRRI TRIGA reactor and its associated equipment. Section 8 of the LAR Rev. 1 describes how access to the AFRRRI complex is controlled.

During the audit (Ref. 5), the NRC staff observed the physical locations of the equipment, how AFRRRI control access to the control console and I&C systems proposed in the LAR, and the measures used to ensure access to the reactor controls are limited to authorized personnel. In addition to limiting physical access, AFRRRI has implemented two equipment-level access restrictions to prevent unauthorized access to the reactor controls, including key locks and password control.

The magnet power key switch located on the reactor control panel prevents unauthorized operation. In order to energize the electromagnet, the facility interlocks must be satisfied, and the magnet key switch must be turned to the "On" position. The AFRRRI Interim Reactor Facility Director controls the key, which remains in their office.

Section 8 of the LAR, Rev. 1, describes the login/password controls for the AFRRRI reactor. The licensee stated with (Ref. 4) that facility procedures require two access levels to the control

console. One level is for operators and the other for the system administrator. Each operator would have a login and password assigned to them. AFRRRI explained that this restriction to access the control console is not for safety, but instead this protection is only provided for accounting purposes (i.e., operator statistics, such as power, login time, operation time, etc.). The NRC staff observed the operator statistics in the UIT display.

During the audit, the NRC staff observed the location of the Universal Serial Bus (USB) ports, secure digital (SD) card or CD recorder provided for in the control console. These ports were not locked or secured at the time; however, a subsequent photo was provided and reviewed during the virtual part of the audit. These photos show that the ports were secured as part of the audit. The AFRRRI TRIGA Operations & Maintenance (O&M) Manual, Section 2.1.1.2, states that remote computers should not be connected to these computers because connecting remote computers would allow remote access and control of the reactor. AFRRRI staff stated that they rely on the restriction to access the control room for preventing access to these ports. Further, AFRRRI explained that operators cannot change anything that impacts the safety of the system because the reactor trips are all analogs and can only be changed at the respective NI modules located outside the control room.

During the audit, the NRC staff also visually observed the location of the cabinets for the control console. The NRC staff observed the control console includes a printer for operators to print trends and historical data. The printer is within the console cabinet and can be accessed through the backdoors. Also, through the cabinet backdoors, the operators could access cables and wiring to and from the control console. These backdoors are all locked.

Also during the audit, the NRC staff visually confirmed the location of the DAC, FIS cabinet, and MCC in the reactor room. The NRC staff confirmed that the NIs are housed in the DAC, and they do not connect to any external network. Additionally, AFRRRI stated that the NI's firmware/software cannot be modified by AFRRRI staff. All of these cabinets are locked.

The NRC staff noted that all keys are kept by the AFRRRI Interim Reactor Facility Director. Further, AFRRRI does not have a procedure to manage and control access to these keys, nor do they have a log to record the use of these keys. This practice is consistent with other research reactors and is acceptable.

Based on its review of the application and audit observations, the NRC staff finds that potential I&C access controls vulnerabilities (physical and electronic), including the upgraded nuclear instrumentation modules (e.g., NLW-1000), are adequately addressed for the I&C safety systems and software and the administrative controls prevent/limit unauthorized physical and electronic access to the I&C systems. Accordingly, the NRC staff finds the AFRRRI I&C access controls are acceptable.

3.9.3. Conclusion on Access Controls

The NRC staff evaluated the access control for the I&C systems in accordance with the design acceptance criteria of Chapter 7 of NUREG-1537, Part 2, including acceptance criteria from the guidance and industry standards referenced by Chapter 7 of NUREG-1537, as listed in Section 2 of this SE. Based on its evaluation of the information presented above, the NRC staff concludes:

- The I&C design incorporates the reactor key protection and prevents unauthorized reactor operation by requiring use of a key at the reactor control console. Additional

electronic authentication prevents access to, and control of, the control console to help ensure operation of the reactor is restricted to authorized personnel.

- The AFRRRI facility includes physical means to limit access to NIs, DAC, FIS, and control console. In addition, the software access authorization of the control console ensures that if the reactor controls are accessed or modified by unauthorized personnel, AFRRRI staff could retrieve this information to determine who did it.

3.10. Evaluation of AFRRRI Digital Upgrade Development Process

This section of the SE documents the NRC staff's evaluation of the design and development for the digital upgrade of the proposed I&C systems using the acceptance criteria guidance in Chapter 7 of NUREG-1537, Part 2 including acceptance criteria from the guidance and industry standards referenced by Chapter 7 of NUREG-1537, as listed in Section 2.0 of this SE.

In the proposed SAR, Rev. 1, AFRRRI proposed replacing the I&C system for its TRIGA reactor. For this evaluation, the NRC staff reviewed the design and development process established by the licensee and its I&C systems vendor, General Atomics-Electronics Systems Inc. (GA-ESI).

3.10.1. Quality Assurance

A robust QA program and managerial and administrative controls are necessary to help ensure that the system can perform its required functions. Section 50.34(b)(6)(ii) of 10 CFR, requires a description in the SAR of managerial and administrative controls to be used to help ensure safe operation. Section 7.2.1 of NUREG-1537, Part 1 recommends that all systems and components of the I&C systems should be designed, constructed, and tested to quality standards commensurate with the safety importance of the functions to be performed. Section 12.9 of NUREG-1537, Part 1 states the applicant should consider the guidance in Regulatory Guide (RG) 2.5 and ANSI/ANS-15.8-1976 in developing quality assurance programs for non-power reactors. The general requirements for establishing and executing a quality assurance program for the testing, modification, and maintenance of research reactors in ANSI/ANS-15.8-1995, which is endorsed by RG 2.5, provide an acceptable method for complying with the quality requirements of 10 CFR 50.34. However, ANSI/ANS-15.8-1995 recognizes that the described controls are integral to the management of a facility and that it is not necessary to establish a separate QA program for a facility upgrade such as an upgrade to the I&C systems. ANSI/ANS-15.1-1990 provides guidance on documenting the managerial and administrative controls in the facility TSs.

In Section 1 of the LAR, Rev. 1, AFRRRI explained that the proposed I&C system uses the General Atomics (GA) I&C system, which includes the latest components and features to improve reactor operation, while maintaining prior system architecture, operation, and protection of the TRIGA reactor. Further, the performance of the proposed I&C systems are assured through both the AFRRRI's quality assurance plan and the vendor's quality assurance plan. The proposed I&C system was designed and manufactured in accordance with ANSI/ANS-15.15-1978, "Criteria for the Reactor Safety System Research Reactors." The I&C system was also validated by a comprehensive verification and validation testing program, as described in Section 3.10.4 of this SE.

In Section 7.1.1 of the proposed SAR, the licensee noted that because there are no special requirements of the AFRRRI reactor, there are no additional quality assurance requirements needed to accommodate any unusual or unique aspects of the design of the Reactor I&C

system. As stated above, General Atomics provided the new TRIGA control system for AFRRRI. This included the control console, NP-1000 channel, NPP-1000 channel, NFT channel, NLW-1000 channel, rod control and rod drives, scram loop, DAC, FIS, ER control boxes, Primary Water Temperature Measuring Channels, and Pool Level Measuring Channel. The licensee described GA's quality assurance and testing program for each component replaced in the proposed SAR, Rev. 1 (i.e., Section 1.1.7, Quality Assurance). GA developed and tested the equipment provided in accordance with its Quality Assurance Manual and Quality Assurance Procedures, which adhere to 10 CFR Part 50, Appendix B, and ASME NQA-1-2008 and ASME NQA-1 Part II. GA also followed its Software Quality Assurance Verification and Validation Plan. ASME NQA-1 is generally approved for incorporation by reference in 10 CFR 50.55(a)(1)(v) for power reactor quality programs. NRC regulations do not require the use of NQA-1 at research reactors, such as AFRRRI. These vendor qualifications for the proposed I&C system generally meet or exceed the applicable non-power reactor guidance of ANSI/ANS-15.8-1995 and NUREG-1537, Part 2 with regards to the proposed I&C system.

During the audit (Ref. 5), the NRC staff observed GA's QA manual, procedures, documentation, and testing records prepared for the AFRRRI proposed I&C system. These documents are described in the following sections of this SE.

The AFRRRI QA program is implemented in accordance with ANSI/ANS-15.8-1995. The licensee stated with (Ref. 4) that if a change to the I&C system is desired, then they will contract with GA to provide those services and as such use GA's QA procedures and programs as allowed by ANSI/ANS-15.8-1995.

Because GA uses a newer version of NQA-1, the NRC staff compared the referenced versions of NQA-1 to the 10 CFR Part 50, Appendix B requirements and to ANSI/ANS-15.8-1995 and finds that the NQA-1 requirements cited by GA meets or exceeds the guidance in ANSI/ANS-15.8-1995. Based on the information provided and reviewed, the NRC staff concludes that the QA program, which relied on the vendor's QA program for the design and development of the I&C system follows the guidance for quality assurance in ANSI/ANS-15.8-1995 and is acceptable. Additionally, the QA provisions for the design, development and test of the I&C system meets the 50.34(b)(6)(ii) requirement that managerial and administrative controls be used to assure safe operation. Accordingly, the NRC staff finds the QA program acceptable.

3.10.2. Configuration Management

ANSI/ANS-15.8-1995 recommends that equipment that requires configuration control be identified, and that management be responsible for establishing and maintaining proper configuration and provide written authorization of any changes to safety-related items.

The LAR, as supplemented states that GA used its TRIGA Software Configuration Management Plan (SCMP). During the audit, the NRC staff looked at the SCMP. This TRIGA SCMP establishes the GA-ESI program be followed for checking, documenting, and reviewing changes to instrumentation software for the proposed I&C system. Based on the information reviewed during the audit (Ref. 5), the NRC staff concludes that the proposed I&C system was developed in accordance with General Atomics' QA plan and procedures and was properly documented and certified by the licensee.

GA-ESI installed the TINA (TRIGA reactor emulator and training tool) in the control console. This tool can be used to update, develop, test, evaluate and train AFRRRI staff. During the audit,

AFRRI explained that the staff does not have access to this tool to make changes to the system. Further, the licensee stated with (Ref. 4) that the configuration of the NIs can only be performed by GA-ESI and the AFRRI staff do not have access to make changes (NIs are housed within the DAC, which is locked).

In the control console, the operator can see the system version in the Site/Operator box in the right-side graphic display. During the audit, the NRC staff visually confirmed that this information is available at all times. Also, during the audit, the NRC staff looked at the GA-ESI "Acceptance Test Procedure, Console Assembly, AFRRI TRIGA." The NRC staff observed that the current software version in the control console is the same that was used for the acceptance testing. Procedure OP-4.0-140, "Design Control," Revision R establishes the configuration management control the design.

Based on the information reviewed, the NRC staff finds that the design and development of the proposed I&C system for the AFRRI TRIGA reactor uses a configuration control that appropriately traces changes to safety system software from point of origin to implementation and that the licensee has a program to ensure installation of the correct version of the software. Therefore, the NRC staff concludes that the AFRRI configuration management of the proposed I&C system meets the acceptance criteria for configuration management in ANSI/ANS-15.8-1995, which is referenced in Section 12.9 of NUREG-1537 and endorsed by RG 2.5.

3.10.3. Design and Development Process

For the proposed I&C system, General Atomics developed a "Software Development Plan" (SDP) to describe planning, organization, roles and responsibilities, process and procedures, methods, tasks, products, and reviews used to develop the AFRRI TRIGA software. GA used this plan for the development of the software for the TRIGA control console and nuclear channels.

During the audit, the NRC staff looked at the SDP. The SDP defines the system development lifecycle to follow, as well as the activities, tasks, and deliverables for each phase. This SDP is also used to tailor the standard Software Engineering activities to fit the needs and constraints of this project.

GA-ESI developed the Conceptual FRS (Ref. 15) for the replacement of the old AFRRI monitoring, control, and safety systems. This document defines operation, characteristics, and features for the proposed I&C system. The NRC staff reviewed the FRS and finds that the document details the desired system capabilities, conditions, and constraints to replace the old I&C system.

Using the FRS, GA-ESI defined the system requirements in its "System Requirements Specification" (SyRS). During the audit (Ref. 4), the NRC staff looked at the SyRS. This document includes description of the proposed I&C system and its components. It also defines the requirements to achieve the system capabilities, conditions, and constraints defined in the FRS. Based on the information reviewed during the audit, the NRC staff confirmed that the functional requirements defined in the FRS, including potential security vulnerabilities, were acceptably translated in this document, to further define the design of the proposed I&C systems.

Therefore, the NRC staff concludes that the proposed I&C system for the AFRRI TRIGA reactor meets the design acceptance criteria in Chapters 3, 7, 8, 13, and 14 in NUREG-1537, Part 2 including acceptance criteria for hardware and software for computerized systems applicable to non-power reactor DI&C systems in the guidance and industry standards for digital upgrades referenced in Chapter 7 of NUREG-1537, Part 2.

3.10.4. Software Quality Assurance and Verification and Validation

As part of the software development process, GA-ESI prepared a Software Quality Assurance and Verification and Validation Plan to define the software QA requirements for the I&C system replacement. This document also describes the verification and validation (V&V) tasks and activities to be performed throughout all phases of the software development process and products.

This plan defined the V&V activities and associated requirements, roles and responsibilities, development activities, defect reporting, and corrective actions followed during the development of the I&C system for the AFRRI TRIGA reactor. The NRC staff reviewed this document during the audit (Ref. 5).

The licensee and its vendor performed acceptance tests for all components of the proposed I&C system. The audit report details the activities and results obtained during these tests. During the audit, the NRC staff confirmed that the tests were successfully completed. Then, GA-ESI performed a factory acceptance test (FAT) to demonstrate the replacement I&C system meets the system requirements specified in the scope of work and the functional requirement specifications. The FAT also demonstrated the features, operation, and safety aspects of the control console to show proper behaviors and responses of the software and hardware. During the audit, the NRC staff confirmed that the tests were successfully completed. The NRC staff also reviewed examples of defect reporting created during acceptance tests. These are described in the audit report. The NRC staff noted that two items found during the FAT of the control console were not addressed. In Ref. 16, the licensee explained why, even though these items were not resolved, they were found acceptable because the items would not affect the performance of the software.

The software quality assurance verification and validation plan require the preparation of a software quality assurance report (SQAR). In Ref. 16, the licensee stated that this report was not prepared. However, the NRC staff determined that the testing documents (e.g., FAT) identified problems and corrected methods that illustrate the information that would have been part of a SQAR, effectively creating equivalency.

After the FAT was completed, the licensee performed the tests identified in the "Site Acceptance Test" (SAT). The SAT was performed to demonstrate that the replacement I&C system was properly installed for operation at AFRRI, meets the technical, functional, and operational requirements, and verifies that the system can be used to operate the AFRRI TRIGA reactor. The audit report details the activities and results obtained during SAT. During the audit, the NRC staff reviewed the test report and observed that all tests were passed.

Based on the information reviewed, the NRC staff finds that this plan established the measures, activities, roles, and responsibilities for the development of a robust software. The NRC staff also finds that the testing program adequately tests all portions of the system design to ensure the proposed I&C system meets its design requirements and acceptance criteria that applies to non-power reactor DI&C systems from the guidance and industry standards for digital upgrades referenced in Chapter 7 of NUREG-1537, Part 2 (Ref. 6).

3.10.5. Conclusion for Digital Upgrade Development Processes

The NRC staff evaluated the I&C design, including the development, implementation, and testing process, in accordance with the design acceptance criteria associated with performing digital upgrades in Chapter 3, 7, 8, 12, 13, and 14 in NUREG-1537, Part 2 including the applicable acceptance criteria for non-power reactor DI&C systems in the guidance and industry standards for digital upgrades referenced in Chapter 7 of NUREG-1537, Part 2.

The NRC staff finds that the development, implementation, and testing process for the I&C system design produced a reliable and fail-safe system which is acceptable for use in AFRRRI. Specifically, the NRC staff concludes that the proposed I&C system provides reasonable assurance that AFRRRI can operate safely without exceeding the safety limit established in the TSs, based on the following:

- The I&C design adequately documents the design bases and the functional characteristics of the safety system hardware and software, and the requirement specifications are properly described for each requirement.
- The quality of the software and hardware components follows the established non-power reactor guidance using a graded approach consistent with the appropriate degree of safety importance and reliability goals warranted for the I&C system. The replacement, modification, or changes to the facility I&C systems meet or exceed the requirements of the original systems or components.
- The I&C design adequately documents the validation and verification of the safety system software development activities, and the documentation exists to show that the V&V tasks will be successfully accomplished for the I&C system to verify conformance of the structures, systems, and components to the specified requirements.
- The I&C design adequately documents that the configuration management program appropriately traces changes to safety system software—from their point of origin to implementation—and addresses any impacts on system safety, control console, or display instruments.
- The I&C design provides assurance that the required computer system hardware and software are installed in the appropriate system configuration and the licensee has a management program to ensure that the correct version of the software/firmware is installed in the correct hardware components.

3.11. Technical Evaluation of Proposed Changes to Technical Specifications

The AFRRRI TSs provide the definitions, safety limits, limiting safety system settings, LCOs, SRs, design features, and administrative controls required to operate the facility. As part of the LAR, as supplemented, the licensee proposed changes to the AFRRRI TSs primarily to correspond to design and operational changes resulting from the replacement of the I&C systems. The NRC staff reviewed the format and content of the proposed TSs for consistency with the guidance in NUREG-1537, Part 1, Chapter 14, and Appendix 14.1, and ANSI/ANS-15.1-2007. Consistent with NUREG-1537, Part 2, Chapter 14 (Ref. 6), acceptance criteria, the NRC staff also

evaluated the proposed TS revisions to determine whether the proposed AFRR I TSs meet the requirements in 10 CFR 50.36.

The licensee also proposed additional TS changes that corrected terminology references and clarified procedural requirements. The NRC’ staff’s technical evaluation follows each description, in the discussion below.

3.11.1 TS 3.2.2, “REACTOR SAFETY SYSTEMS,” Table 2

To support the DI&C upgrade, AFRR I requested revisions to TS 3.2.2, Table 2, “Minimum Reactor Safety System Scrams,” to add a second watch dog scram circuit, change the names of the two watchdog timer scram circuits, from “DAC and CSC” to “UIT and CCS” and add an AC Power Loss scram circuit.

Prior to the upgrade, there was one watch dog timer, and it controlled both the DAC and the CSC. After the upgrade, there would be two watchdog timers, one controlling the User Interface Terminal computer and the other controlling the console computer system (CCS) computer, for both “Effective Modes” of operation: steady state and pulse. The maximum set point for each channel would be 15 seconds before actuating a scram.

The new console receives power from an uninterruptible power supply (UPS), which includes power to the control rod magnets. To ensure the reactor scrams when offsite power is lost, the licensee introduced a new scram to occur on loss of AC power supply to the UPS.

The proposed TS changes set forth below are denoted using **bold** to indicate addition and ~~strikethrough~~ to indicate deletion.

Table 2. Minimum Reactor Safety System Scrams

Channel	Maximum Set Point	Effective Mode	
		Steady State	Pulse
Fuel Temperature	600°C	2	2
Percent Power, High Flux	1.1 MW	2	0
Console Manual Scram Button	Closure switch	1	1
High Voltage Loss to Safety Channel	20% Loss	2	1
Pulse Time	15 seconds	0	1
Emergency Stop	Closure switch	3	3
(1 in each exposure room, 1 on console)			
Pool Water Level	14 feet from the top of the core	1	1
Watchdog (DAC to CSC)	On digital console	1	1
Watchdogs (UIT and CCS)	15 seconds	2	2
AC Power Loss	15 seconds	1	1

The new instrumentation and control system would have two watchdog timers (WDTs) one attached to the UIT and the other attached to the CCS. These WDTs would detect issues such as CPU latch-up, control system faults, control system faults, wiring/cabling failure, unauthorized tampering, unanticipated software conditions, communications problems, or power

failures. If either the UIT or CCS computers fail to send a keep-alive signal to their respective watchdog timers, the WDT times out and causes a scram to occur. If the WDTs lose power, a scram will also occur. The WDTs also cause a scram if the computer software stops operating properly. The UIT and CCS are independent from the nuclear instrumentation that protects against exceeding the safety limit—the NIs that initiate protective scrams are completely analog instruments.

In its proposed changes to the TSs (Ref. 18), the licensee stated that even if the worst case scenario occurred, in which the uncontrolled withdrawal of a control rod caused by a nonresponsive system resulting in a positive reactivity insertion event, the reactor would remain below the maximum reactivity limit of $\beta_{3.50}$. Since the design of the WDTs is to shut down the reactor if the digital control system fails and alert the operator, and even if it didn't work, the 15 seconds is adequate and matches the setpoint for the pulse timer. If the WDTs didn't activate, even though communication with the computers would be lost, the scrams activated by the analog nuclear instruments controlling the reactor would not be affected, since they are analog and separate from the digital system.

The NRC staff finds that the safety of the reactor will be protected even if the WDTs fail and that the proposed changes to TS 3.2.2, Table 2 will not result in risk to the health and safety of the public.

AC Power Loss Scram

The AFRRRI reactor was designed for fail-safe passive shutdown by a reactor scram in the event of the loss of AC Power. The licensee proposed the addition of an uninterruptible power supply, which would protect the reactor instrumentation and control system and provide for an orderly shutdown of the console computers if the reactor and control room were to suffer the loss of AC Power. However, with the addition of the proposed UPS, in the event of AC Power loss to the facility, the UPS provides backup power automatically to the reactor control system, but the UPS would provide AC power to the reactor control system for at least 15 minutes, thereby it would keep the reactor running. To prevent this situation, the licensee proposed a scram in the event of loss of AC power. The AC power loss scram would generate its own scram and open a contact on the UPS. The addition of the AC power loss scram, at 15 seconds after the loss, provides an automatic scram that defeats the effect of the UPS. The end result is that in the event of AC power loss, the UPS kicks into protect the I&C system, and within 15 seconds of the loss the AC power loss scram actuates. Note that in the event of a power loss, the licensee is not authorized to operate the reactor without the building and reactor support systems, such as lighting and ventilation; accordingly, if the lights shut off, the reactor operator is required to scram the reactor. But if the reactor operator does not scram the reactor within 15 seconds, the proposed changes will result in the reactor scrambling due to AC Power Loss. In summary, the proposed TS condition precludes operation of the reactor when there is no AC power to the building. The setpoint for the AC Power Loss scram is 15 seconds, which is sufficient for protecting the reactor systems. Because other systems, including the pumps to the primary and secondary cooling systems, ventilation, are still required by the TSs, the reactor cannot run without AC power and the addition of an AC power loss scram is a necessary adjunct to the TS change introducing the UPS.

The guidance in Section 8.1 of NUREG-1537, Part 2 states that TSs should be provided to ensure operability commensurate with power requirements for reactor shutdown and that the design of the electrical power system provides that in the event of the loss or interruption of AC power, the reactor can be safely shut down. Based on the NRC staff's review of the proposed

AFRRI TS 3.2.2. requirement, to preclude operation of the reactor without electrical power to the building, the NRC staff finds that the AFRRI TS 3.2.2 is consistent with the guidance in Section 8.1, "Normal Electrical Power Systems" in NUREG-1537, Part (Ref. 6). The NRC staff also finds that 15 seconds is a reasonable amount of time for the AC Power Loss Scram to actuate and preclude operation of the reactor without AC power. Since the safety functions do not rely on DI&C, this action and its timing are reasonable.

Based on the above, the NRC staff concludes that proposed TS 3.2.2 establishes the lowest functional capability or performance levels of equipment required for safe operation of the facility consistent with the SAR. Therefore, TS 3.2.2 meets the 10 CFR 50.36(c)(2) requirement for an LCO and is acceptable.

3.11.2. TS 3.2.2, "REACTOR SAFETY SYSTEMS," Table 3

To support the DI&C upgrade, the licensee requested revisions to TS 3.2.2, Table 3, "Minimum Reactor Safety System Interlocks"

- 1) to remove the reference to NM-1000 since this NI channel is no longer used and is no longer installed in the reactor. The NM-1000 has been replaced by two channels, NMP-1000 and NLW-1000.
- 2) to remove "operational channel" because it is no longer applicable for the new instrumentation, and replace it with linear power channel or log power channel as follows. For the NMP-1000, the TS change would replace the term "operational channel" with "Linear Power Channel," and for the NLW-1000, the TS change would replace the term "operational channel" with "Log Power Channel."
- 3) to change the units for the low source interlock setpoint, from counts per second to watts.

With the previous I&C system, the operational channel, NM-1000, used to have a multi-range linear component and a wide-range log component and utilized the signal from one fission chamber which covered the neutron flux range from source to full power. With the new I&C system, the linear portion of the operational channel has been replaced by NMP-1000, which is a multi-range channel for the range source through full power. The logarithmic portion has been replaced by NLW-1000, which is a logarithmic channel capable of indicating from source range through full power. The units of the output of the NMP-1000 channel are current, displayed in watts, not counts per second. The NLW-1000 displays percent full power.

In the proposed TS 3.2.2, Table 3, the " 1×10^{-5} watts" setpoint of the NMP-1000 replaces "count rate below 0.5 cps" setpoint because the NMP-1000 uses a compensated ion chamber and the output is displayed in watts. The 1×10^{-5} watts is below the anticipated source level with the Am Be source installed and is above the anticipated source level if the source were removed; therefore, the set point ensures proper instrumentation response prior to rod motion. In addition, the setpoint ensures sufficient source neutrons are present to provide a signal to the startup channel.

The proposed TS changes set forth below are denoted using **bold** to indicate addition and ~~strike through~~ to indicate deletion.

Table 3. Minimum Reactor Safety System Interlocks

Action Prevented	Effective Mode	
	Steady State	Pulse
Pulse initiation at power levels greater than 1 kW		X
Withdrawal of any control rod except transient		X
Any rod withdrawal with count rate below 0.5 cps power level below 1×10^{-5} watts as measured by the operational channel Linear Power Channel (NMP-1000)	X	X
Simultaneous manual withdrawal of two standard rods	X	
Any rod withdrawal if high voltage is lost to the operational channel Log Power Channel (NLW-1000)	X	X
Withdrawal of any control rod if reactor period is less than 3 seconds	X	
Application of air if the transient rod drive is not fully down. This interlock is not required in Square Wave mode.	X	

* Reactor safety system interlocks shall be tested daily whenever operations involving these functions are planned

The NRC staff finds that the changes proposed for TS 3.2.2, Table 3, for the reactor safety system interlocks do not affect the functions of the instruments and that the new linear power channel and log power channel have same function and performance as the NM-1000 which these replaced. Sections 3.3.2 and 3.2.3 of this SE provide the technical evaluation. Since the new instruments have equivalent functionality, performance, and quality as the old instrument, the NRC staff finds the change acceptable. The change from cps to watts is appropriate and is therefore acceptable.

3.11.3 TS 4.2.2., “REACTOR SAFETY SYSTEMS,” Specification b

To support the DI&C upgrade, the licensee requested a revision to TS 4.2.2., Specification b, first, to delete one instance of the repeated words “of each,” and second, to explicitly state that the channels to be tested are the reactor safety system channels as specified in TS 3.2.2 Table 2 and Table 3 with the exceptions of the exposure room emergency stop scrams and AC power loss scrams.

Proposed TS 4.2.2, Specification b., states:

A channel test of each of each of the reactor safety system channels in Table 2 and Table 3 with the exception of the exposure room emergency stop and AC power loss scrams for the intended mode of operation shall be performed weekly, whenever operations are planned.

For the first change, removing the extra “of each” is an editorial change that corrects a typing error. This change does not impact the intention of the specification, and has no impact on the reactor’s structures, systems, or component. Therefore, NRC staff finds there is no adverse impact to reactor safety.

The second change relates to TS 3.2.2 Table 2 and Table 3. The current TS does not state which channels the licensee considers the “reactor safety system channels.” The change will specify which channels are “reactor safety system channels.”

The NRC staff finds that this TS change is acceptable since a failure or malfunction of the pushbuttons would continue to cause a scram and the emergency stops and AC power loss are not “reactor safety system channels.” The NRC staff also finds the licensee’s proposed changes meet the 10 CFR 50.36(c)(2) requirement that LCOs provide the lowest functional capability or performance levels of equipment required for safe operation of the facility consistent with the SAR. Therefore, the NRC staff concludes that proposed changes for Tables 2 and 3 are acceptable.

3.11.4 TS 4.2.2., REACTOR SAFETY SYSTEMS, Specification c

AFRRI requested a revision to TS 4.2.2., Specification c, first, to add that the verification of the setpoints for the high voltage loss to the safety channel scrams be part of the channel calibrations, and second, to remove “NM-1000.”

Proposed TS 4.2.2., Specification c., states:

Channel calibration, **including verification of the setpoints for the high voltage loss to safety channel scrams**, shall be made of the NP, NPP, NM1000, NLW, NMP or any other console instrumentation designated to provide direct power level information to the operator, annually not to exceed 15 months.

The NRC staff finds this TS change is acceptable since it would demonstrate operability of a scram signal that is part of the scram loop. The periodicity is unchanged. The NRC staff finds that adding the requirement for verification of the setpoints provides clarity to the TS surveillance and is consistent with the 10 CFR 50.36 (c)(3) requirement that SRs relating to test, calibration, or inspection assure that the necessary quality of systems and components is maintained and is acceptable. Second, since the NM-1000 has been removed and uninstalled and is no longer needed, the NRC staff finds the removal of reference to NM-1000 acceptable.

3.11.5 TS 4.2.2., “REACTOR SAFETY SYSTEMS,” Specification e

The licensee requested a revision to TS 4.2.2., Specification e, to specify that the exposure room emergency stop and AC power loss scrams shall be tested annually.

Proposed TS 4.2.2., Specification e., states:

The **exposure room emergency stop and AC power loss** scrams shall be tested annually, not to exceed 15 months.

This surveillance requirement helps ensure the quality of the structures, systems, and components to ensure that the specifications of the LCO TS 3.2.2, Table 2, are capable of performing the intended safety function. The licensee stated in the April 4, 2022, submittal, that AFRRI’s emergency stops are industry standard turn-to-reset pushbuttons that are wired to be normally closed (i.e., opening the circuit causes a scram). A break or malfunction of the circuit would cause a scram. The contact block for the emergency stop has an electrical life rating of 1,000,000 operations, so failure is not credible. Annual testing is therefore reasonable. Note that the emergency stop scram at the console continues to be tested weekly.

Annual testing for the AC power loss scram is reasonable since AFRRRI staff desires to minimize unnecessary cycling of power to the UPS. The NRC staff's evaluation of the AC Power Loss scram is provided in Section 3.11.1 of this SE.

The NRC staff finds that the requested change to TS 4.2.2, Specification e, to test the exposure room emergency stop and AC power loss scrams annually helps maintain the quality of the SSCs and helps ensure that these scrams are capable of performing the intended safety functions. The NRC staff finds that this change is consistent with the 10 CFR 50.36 (c)(3) requirement that SRs relating to test, calibration, or inspection assure that the necessary quality of systems and components is maintained and is acceptable.

3.11.6 TS 4.2.4., "FACILITY INTERLOCK SYSTEM," Specification b

AFRRRI requested a revision to TS 4.2.4., Specification b, to reflect the installation of the core dolly override switch to allow for the movement of the core dolly in region 2 while the lead doors are closed with the use of the core dolly override switch. The change adds to the specification the exception that the core dolly cannot be moved in region 2 with the lead doors closed except during the use of the core dolly override switch.

Proposed TS 4.2.4., Specification b., states:

The core dolly cannot be moved ~~into~~ **in** region 2 with the lead shield doors closed **except during the use of the core dolly interlock override switch.**

Section 3.4 of this SE describes and evaluates the addition of this switch. The NRC staff finds that this change is acceptable because this function existed in the previous system. Further, this addition would demonstrate operation of the interlock system. The NRC staff finds that this change is consistent with the 10 CFR 50.36 (c)(3) requirement that SRs relating to test, calibration, or inspection assure that the necessary quality of systems and components is maintained and is acceptable.

3.11.7 Conclusion on TS Changes

The NRC staff reviewed AFRRRI's proposed TS changes related to the upgrade of the digital instrumentation and control system. Based on its review, the NRC staff finds that the TS changes are based on the system description and performance requirements in the SAR, as revised by the LAR and are consistent with the guidance in NUREG-1537, Part 1, Appendix 14.1. Based on its evaluation of the information presented above, the NRC staff concludes:

- The licensee provided TSs, as required by 10 CFR 50.36(a), are consistent with 10 CFR 50.36(b) and the TSs are derived from the SAR analyses as revised by the LAR, as supplemented.
- The proposed TSs assure that the necessary quality of system components is maintained that facility operation will be within the safety limits, and that the LCOs and SRs will be met as required by 10 CFR 50.36(c)(3) and 10 CFR 50.36(c)(3).

Therefore, the NRC staff concludes that the proposed changes to the TSs provide reasonable assurance that the AFRRRI will be operated as analyzed in the LAR, as supplemented, in a

manner that protects the health and safety of the public. Accordingly, the NRC staff concludes that the proposed changes to the TSs are acceptable.

4.0 ENVIRONMENTAL CONSIDERATION

The amendment changes requirements with respect to the installation or use of facility components located within the restricted area as defined in 10 CFR Part 20 and changes SRs. The NRC staff has determined that the amendment meets the following criteria:

- (i) The amendment involves no significant hazards consideration (10 CFR 51.22(c)(9)(i));

Pursuant to 10 CFR 50.92(c) the Commission may make a final determination that a license amendment involves no significant hazards consideration if operation of the facility, in accordance with the amendment, would not:

- (1) Involve a significant increase in the probability or consequences of an accident previously evaluated (10 CFR 50.92(c)(1));

The license amendment allows the upgrade of the reactor console and instrumentation for the DI&C system. As discussed in Section 3.0 of this SE, which includes the NRC staff's evaluation of the design bases and criteria for the RCS, RPS, display system, and radiation monitors, no substantive changes were made to the SL or LSSS setpoints in the proposed LAR. The shutdown margin and calculation methodology were not modified and the shutdown margin requirement previously approved by the NRC is maintained. The licensee used the same conservative factors for instrument error and delay time as previously approved by the NRC, even though the DI&C system upgrade allows for a faster response time and is more accurate. The new system does not include the ability to bypass RCS interlocks. The new system includes diverse means to scram the reactor. The RPS is always capable of shutting down and maintaining safe shutdown of the reactor. Consequently, the amendment does not change the accident analyses previously approved by the NRC for the AFRRRI reactor.

For these reasons, there is no significant increase in the probability or consequences of an accident previously evaluated.

- (2) Create the possibility of a new of different kind of accident from any accident previously evaluated (10 CFR 50.92(c)(2));

The NRC staff evaluated the licensee's analyses of the credible accident scenarios as part of the license renewal (Ref. 20) for the AFRRRI reactor and the staff previously found the results of these accident analyses to be acceptable when it renewed the license. The existing TS SL and LSSS are unchanged by the amendment and operation of the facility remains bounded by the previous accident analyses found to be acceptable by the NRC staff when it renewed the license for the AFRRRI reactor. Proposed changes to the LCOs do not change the lowest functional capability or the performance levels of equipment required for safe operation of the facility. Additionally, the proposed DI&C upgrade does not fundamentally change the manner in which the AFRRRI reactor is operated. For these reasons, the amendment does not

create the possibility of a new or different kind of accident from any accident previously evaluated.

(3) Involve a significant reduction in a margin of safety (10 CFR 50.92(c)(3))

The existing and proposed AFRRI TSs will continue to ensure the ability to safely operate the AFRRI reactor. As discussed in Section 3.0 of this SE, the proposed TSs include provisions that would initiate protective action sooner and provide a greater safety margin and no proposed changes adversely affect the safety margins. Because the facility personnel and the public health and safety will continue to be adequately protected, the amendment does not involve a significant reduction in a margin of safety.

(ii) There is no significant change in the types or significant increase in the amounts of any effluents that may be released offsite (10 CFR 51.22(c)(9)(ii)); and

The DI&C upgrade and TS changes do not change the reactor source term, the fission products generated, or the amounts of any effluents that may be released offsite because there is no change to the AFRRI reactor design and procedures that control radiation sources and potential effluents. In addition, the amendment does not change the potential release paths from the reactor and does not change the AFRRI radiation protection program or radioactive waste management program. For these reasons, there is no significant change in the types or significant increase in the amounts of any effluents that may be released offsite.

(iii) There is no significant increase in individual or cumulative occupational radiation exposure (10 CFR 51.22(c)(9)(iii)).

The amendment does not change the licensed power level or significantly alter reactor operations or requirements. The site perimeter (controlled area) and basic configuration of the AFRRI reactor are unchanged from that approved previously by the NRC staff during license renewal (Ref. 20). The amendment does not change existing administrative controls or the AFRRI radiation protection program for limiting individual or cumulative occupational radiation doses. The TSs and SRs will continue to help minimize individual and cumulative occupational radiation exposure. Accordingly, the resultant occupational dose remains unchanged and well within the regulatory limits of 10 CFR Part 20. For these reasons, there is no significant increase in individual or cumulative occupational radiation exposure.

The amendment also makes editorial, corrective, or other minor revisions to the TSs, none of which have any impact on reactor operation or public health and safety. Accordingly, the amendment meets the eligibility criteria for categorical exclusion set forth in 10 CFR 51.22(c)(9) and 51.22(c)(10)(v). Pursuant to 10 CFR 51.22(b), no environmental impact statement or environmental assessment need be prepared in connection with the issuance of the amendment.

5.0 CONCLUSION

The NRC staff reviewed the LAR, as supplemented (Ref. 4), for the modification to upgrade the AFRRI TRIGA reactor's I&C systems to a new all-digital system. The licensee submitted information for the NRC staff to evaluate the LAR in accordance with the NRC's regulations

using the applicable guidance provided in Chapter 7 of NUREG-1537, Part 2. The NRC staff reviewed the safety analyses submitted, which included descriptions of the design, testing, and operation of the proposed DI&C, and conducted an audit (Ref. 5) to gain a better understanding of the information in the LAR, facility status, and the I&C upgrade. The NRC staff found the proposed revisions to Chapter 7 of the SAR Rev. 1 to be appropriate, and the amendment authorizes the licensee to incorporate the revisions into its SAR. The NRC staff finds that the licensee's request to upgrade the I&C systems for its TRIGA reactor, as discussed in this SE, and the proposed changes to its TSs to be acceptable. On this basis, the NRC staff concludes that the new I&C systems are acceptable because they are designed in accordance with AFRRI's design basis and design criteria, and will allow the TRIGA reactor to be safely operated, as analyzed in the LAR, as supplemented (Ref. 4); and that adherence to the proposed TSs will limit the likelihood of malfunctions as discussed in this SER.

The NRC staff has concluded, based on the considerations discussed above, that (1) there is reasonable assurance that the health and safety of the public will not be endangered by operation in the proposed manner, (2) there is reasonable assurance that such activities will be conducted in compliance with the Commission's regulations, and (3) the issuance of the amendment will not be inimical to the common defense and security or to the health and safety of the public.

Principal Contributors: R. Alvarado, NRR
J. Ashcraft, NRR
P. Boyle, NRR
M. Takacs, NRR
C. Montgomery, NRR

Date: June 27, 2022

6.0 TABLE OF ACRONYMS

10 CFR	Title 10 of the <i>Code of Federal Regulations</i>
AC	Alternating Current
A/D	Analog to Digital
ADAMS	Agencywide Documents Access and Management System
AFRRI	Armed Forces Radiology Research Institute
ANSI/ANS	American National Standards Institute/American Nuclear Society
CAMs	Continuous Air Monitors
CET	In-core Experiment Tube
CCS	Console Computer System
CSC	Control System Console
COTS	Commercial Off the Shelf
cps	Counts per second
CRD	Control Rod Drive
CRDM	Control Rod Drive Mechanisms
DAC	Data Acquisition Cabinet
DC	Direct Current
DI&C	Digital Instrument and Controls
DOD	U.S. Department of Defense
EMI/RFI	Electromagnetic Interference/Radio Frequency Interference
ER	Exposure Room
FAT	Factory Acceptance Test
FIS	Facility Interlock System
FRS	Functional Requirements Specification
GA	General Atomics
GA-ESI	General Atomics -Electronics Systems Inc.
GUI	Graphical User Interface
HLA	High Level Assembly
HMI	Human Machine Interface
HVAC	Heating, Ventilation, and Air Conditioning
IEEE	Institute of Electrical and Electronics Engineers
IFE	Instrumented Fuel Element
I&C	Instrument and Controls
I/O	Input/Output
kW	Kilowatt
LAR	License Amendment Request
LCD	Liquid Crystal Display
LCO	Limiting Conditions for Operation
LED	Light Emitting Diode

LSSS	Limiting Safety System Setting
mA	Milli Amp
MCC	Motor Control Centers
MW s	Megawatt Seconds
MWt	Megawatt Thermal
NI	Nuclear Instruments
NRC	U.S. Nuclear Regulatory Commission
NVT	Network Virtual Terminal
PWA	Printed Wiring Assembly
QA	Quality Assurance Program
QAP	Quality Assurance Plan
RAMs	Radiation Air Monitors
RCA	Radio Corporation of America
RCS	Reactor Control System
Rev.	Revision
RMS	Radiation Monitoring System
ROX	Reactor Permissive
RPS	Reactor Protection System
RTD	Resistive Temperature Detector
RWI	Rod Withdrawal Inhibitor or Interlock
RWP	Rod Withdrawal Prevent
SAR	Safety Analysis Report
SAT	Site Acceptance Test
SCMP	Software Configuration Management Plan
SDP	Software Development Plan
SE	Safety Evaluation
SL	Safety Limit
SQAP	Software Quality Assurance Plan
SR	Surveillance Requirement
SYRS	System Requirement Specifications
TRIGA	Training, Research, Isotopes, General Atomics
TS	Technical Specifications
UIT	User Interface Terminal
UPS	Uninterrupted Power Supply
VAC	Voltage Alternating Current
Vdc	Voltage Direct Current
V/F	Voltage to Frequency
Vrms	Voltage root mean square
V&V	Verification and Validation

7.0 REFERENCES

1. "AFRRI LAR for Digital I&C Upgrade," dated November 10, 2020 (ADAMS Package Accession No. ML20318A338, containing ADAMS Accession Nos. ML20318A339, ML20318A340, ML20318A343, ML20318A346, ML20318A347, ML20318A348, and ML20318A349).
2. "Response to NRC 01/08/2021 Letter re License Amendment Request for Facility Operating License No. R-84 for the AFRRI TRIGA Reactor Docket No. 50-170," dated February 5, 2021 (ADAMS Accession Nos. ML21036A297, and ML21036A300), and dated February 4, 2021 (ADAMS Accession No. ML21036A301) (affidavit).
3. "Transmittal of Proposed changes to the technical specifications in support of the license amendment request for the digital instrumentation and control upgrade for the AFRRI TRIGA Reactor," dated February 11, 2021 (ADAMS Package Accession No. ML20342B840, containing ADAMS Accession Nos. ML21042B841 and ML21042B842).
4. "AFRRI LAR for the Digital Instrumentation and Control Upgrade Revision 1," dated October 28, 2021 (ADAMS Package Accession No. ML20342B840, containing ADAMS Accession No. ML21302A097, ML21302A107, ML21302A100, ML21302A103, ML21302A106).
5. "Armed Forces Radiobiology Research Institute (AFRRI) Digital instrumentation and control (I&C) Audit Report," dated March 29, 2022 (ADAMS Accession No. ML22067A246).
6. NUREG-1537, Parts 1 and 2, "Guidelines for Preparing and Reviewing Applications for the Licensing of Non-Power Reactors, "Format and Content," and "Standard Review Plan and Acceptance Criteria," dated February 1996 (ADAMS Accession Nos. ML042430055 and ML042430048).
7. ANSI/ANS-15.1-1990, "The Development of Technical Specifications for Research Reactors."
8. ANSI/ANS-15.8-1995, "Quality Assurance Program Requirements for Research Reactors."
9. ANSI/ANS-15.15-1978, "Criteria for the Reactor Safety Systems of Research Reactors."
10. ANSI/ANS-10.4-1987, "Guidelines for the Verification and Validation of Scientific and Engineering Computer Programs for the Nuclear Industry."
11. IEEE 7-4.3.2-1993, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations."
12. Regulatory Guide 2.5-1977, "Quality Assurance Program Requirements for Research and Test Reactors."

13. Regulatory Guide 1.152-1996, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants."
14. "Issuance of Amendment No. 19 to Facility Operating License No. 84 – Armed Forces Radiology Research Institute (AFRRI)," dated July 23, 1990, approved the installation of a microprocessor-based instrument and control system (ADAMS Accession No. ML100840590).
15. "Enclosure 3 – USUHS/AFRRI TRIGA Reactor Control System Functional Requirements Specification (Conceptual) - T3S99001-FRS, Rev. A, Redacted," dated November 8, 2021 (ADAMS Accession No. ML21316A036), "Enclosure 4 – Affidavit for Proprietary Information," dated April 27, 2021 (ADAMS Accession No. ML21316A037), "Enclosure 5 - Errata for USUHS/AFRRI TRIGA Reactor Control System Functional Requirements Specification (Conceptual) - T3S990001-FRS Rev A," dated November 8, 2021 (ADAMS Accession No. ML21316A038).
16. "US Dept. of Defense, Uniformed Services Univ. of the Health Sciences - The Armed Forces Radiobiology Research Institute (AFRRI) is Submitting a Supplement to the License Amendment Request for the Digital Instrumentation and Control Upgrade," dated January 7, 2022 (ADAMS Package Accession No. ML22007A263, containing ADAMS Accession Nos. ML22007A264, ML22007A265, and ML22007A266).
17. "AFRRI – LAR – Digital IC – Functional Requirement Specification," dated November 8, 2021 (ADAMS Package Accession No. ML21316A032, containing ADAMS Accession Nos. ML21316A033, ML21316A036, ML21316A036, ML21316A038).
18. "Uniformed Services Univ. of the Health Sciences, Armed Forces Radiobiology Research Institute (AFRRI), Submittal of Supplement to License Amendment Request for the Digital Instrumentation and Control Upgrade (EPID L-2020-NFA-0012)," dated April 4, 2022 (ADAMS Package Accession No. ML22096A279, containing ADAMS Accession Nos. ML22096A280 and ML22096A281).
19. "US Department Of Defense Armed Forces Radiology Research Institute - Regulatory Audit Plan For Digital Instrumentation And Control System Upgrade," dated September 10, 2021 (ADAMS Accession No. ML21253A001).
20. "AFRRI Renewal of Facility Operating License," dated November 30, 2016 (ADAMS Accession No. ML16077A284).
21. "Armed Forces Radiobiology Research Institute (AFRRI) - Supplement to the License Amendment Request for the Digital Instrumentation and Control Upgrade (EPID L-2020-NFA-0012)," dated April 28, 2022 (ADAMS Package Accession No. ML22118A867, containing ML22118A868 and ML22118A869).