7 INSTRUMENTATION AND CONTROL SYSTEMS

This document gives guidance to staff reviewers in the Office of Nuclear Reactor Regulation (NRR) and reviewers under contract to the U.S. Nuclear Regulatory Commission (NRC) for performing safety reviews of applications to construct, modify, or operate a nuclear non-power reactor. The principal purpose of this document is to ensure the quality and uniformity of reviews by presenting a definitive base from which to evaluate applications for license or license renewal. This document also makes information about regulatory matters widely available and helps interested members of the public and the non-power reactor community better understand the review process.

Section 50.34 of Title 10 requires that each application for a construction permit for a nuclear reactor facility include a preliminary safety analysis report (PSAR) and that each application for a license to operate such a facility include a final safety analysis report (FSAR). A single SAR document may be acceptable for non-power reactors, but it must be sufficiently detailed to permit the NRC staff to determine whether or not the facility can be built and operated consistent with applicable regulations.

Instrumentation and control (I&C) systems comprise the sensors, electronic circuitry, displays, and actuating devices that provide the information and the means to safely control the reactor and to avoid or mitigate accidents. Instruments are provided tonmonit6r, indicate, and record such operating parameters as neutron flux density, fuel temperature; coolant flow, temperature, and level; and radiation intensities in selected areas around the reactor. Certain I&C systems will automatically shut down (scram) the reactor when any safety parameter reaches a predetermined setpoint as analyzed in the SAR. I&C subsystems may also be designed to actuate engineered safety features (ESFs) upon the detection of abnormal conditions.

The I&C systems of non-power reactors comprise two basic subsystems-

1. the reactor control system (RCS), interlocks, control console instruments, and radiation monitoring systems necessary and sufficient to operate the reactor under the full range of normal conditions

2. the safety systems [reactor protection system (RPS), ESF actuation system, and radiation safety monitors] added to the I&C systems because of such events as possible accidents, malfunctions, operator error, or release of radioactive material (some components may be a part of both subsystems)

The RPS would be designed to be independent from the RCS if the risks associated with operating a non-power reactor were large. However, non-power reactors can be designed and operated so they pose an acceptably small or insignificant risk to the facility staff the public, and the environment. Such a' facility need not have an RPS independent in all respects from the I&C systems used for normal operations. Most licensed non-power reactors have been designed on the basis of these principles, and the reviewer should anticipate I&C system designs in which subsystems for normal operation and safety subsystems are intermingled. However, the applicant should justify the design of these combined systems and should clearly distinguish and discuss the two functions, noting which components serve both purposes. The consequences of certain malfunctions of the I&C system may render this design approach

unacceptable for high-power test reactors. These cases should be handled individually by the project manager and NRC I&C system experts.

The format and content guide suggests that I&C subsystems and equipment be categorized by the function performed:, RCS, RPS, ESF actuation system, control console and display instrument, or-radiation monitoring instrument The applicant should completely identify the I&C systems in each category. Identification should include such attributes as name, type, function, analog or digital, purpose, and any other distinguishing characteristics.

The I&C system gives the operator information with which to control both the mode of operation and neutron flux (power) level of the reactor. It may also give input to the RCS, allowing changes in reactivity and automatic control of the power level of the reactor by insertion or withdrawal of control rods. Startup is accomplished only by manual control for most non-power reactor designs.

The safety systems (RPS and ESF actuation system) monitor such parameters as neutron flux, fuel temperature, area radiation intensities, and other important parameters to scram the reactor when deemed necessary or to initiate the operation of ESF systems when instruments indicate certain conditions have been met.

The control console and other display instruments present current and past operating parameter and system status information for use in evaluating reactor operating conditions. This information enables the operator to decide on further action, such as when to take manual control of the reactor.

Radiation protection instruments monitor radiation intensities in selected areas that may be occupied in or near the reactor building, or may supply input to the RPS or the ESF actuation system, and may monitor the concentrations or the release of radioactive material in effluent streams from the reactor facility. This information can be used to assess or control personnel radiation exposures.

7.1 Summary Description

Each I&C system for a non-power reactor should be designed to perform functions commensurate with the complexity of the particular facility. Reviewers should anticipate wide variations in design capability and functions of the I&C systems because of the wide variations in such factors as operating thermal power levels and use of non-power reactors. The format and content guide recommends that the SAR should include a summary description of the I&C system: the safety, philosophy, and objectives of its design; the operational characteristics of the reactor that determine or limit the I&C design; and the ways in which the various subsystems constitute the whole and interact to contribute to its essential functions. The format and content guide describes information that should be included in this summary, such as block, logic, and flow diagrams illustrating the various subsystems. The summary description may compare the reactor-specific I&C design with similar ones that NRC has found acceptable for other non-power reactors, including the bases for redundancy and diversity of sensor channels, safety channels, and control elements. The acceptance of the summary description should be based on its completeness in addressing the factors fisted "in the format and content guide.

7.2 Design of Instrumentation and Control Systems

In this section of the format and content guide, the staff discusses various topics that the applicant should include in this chapter of the SAR. The reviewer should confirm that this type of information is in the SAR for each of the I&C systems in its entirety and for each category of subsystem. The SAR should address the following:

- design criteria
- design bases
- system description
- system performance analysis
- conclusion

The remaining sections of this chapter discuss specific information to be included in the SAR for each of the subsystems and how the reviewer should evaluate each subsystem.

7.3 Reactor Control System

Areas of Review

The RCS contains most of the I&C subsystems and components designed for the full range of normal reactor operation. The areas of review for the RCS should include a discussion of the factors requested in Section 7.2 of the format and content guide. The information for the RCS may be presented under the following subtopics:

- nuclear instruments—including all detector channels designed to monitor or measure nuclear radiations, and possibly fuel temperature within the reactor for operational purposes
- process instruments—instruments designed to measure and display such parameters as coolant flow, temperature, or level; fuel temperature; or air flow parameters within or from the reactor room
- control elements—types, number, function, design, and operating features of reactivity control devices other than fuel elements (coordinate with the review of Chapter 4, "Reactor Description")
- interlocks—circuits or devices to inhibit or prevent an action, such as control rod motion, unless a specified precondition exists. Interlocks are intended to protect personnel or other subsystems from harm.

The areas of review for the RCS should also include the following:

- criteria, bases, standards, and guidelines used for the design of the RCS.

- a discussion of the criteria for developing the design bases for the RCS I&C system, including the basis for evaluating the reliability and performance of the I&C systems.
- a review of the criteria for developing the design bases for the RCS I&C system, including the basis for evaluating the reliability and performance of the I&C systems should be provided.
- a review of the design bases of the RCS to Verify that the control systems include the necessary features for manual and automatic control of process variables within prescribed normal operating limits.
- a review to verify that the RCS is not required for safety and that there is a protection system to protect against failures of the control system.
- a description, including logic, schematics, and functional diagrams, of the overall system and component subsystems. The system description with diagrams and auxiliary information should be sufficiently complete to allow a thorough review of all aspects of the RCS including normal /abnormal operation, maintenance, and accident scenarios.
- analysis of the adequacy of the design to establish conformance to the design bases and criteria for reactor power, rate of power change, and pulsing information
- analysis of the adequacy of the design to establish conformance to the design bases and criteria for information on required process variables to control reactor operation
- application of the functional design and analyses to the development of bases of technical specifications, including surveillance tests and intervals
- RCS failure modes to determine if any malfunction of the RCS could prevent the RPS from performing its safety function, or could prevent safe shutdown of the reactor.

Acceptance Criteria

The acceptance criteria together with the use of good engineering practice will help the reviewer to conclude whether the RCS is designed to provide for the reliable control of reactor power level, rate of change of power levels, and pulsing (if applicable) during reactor startup, the fill range of normal operation, and shutdown. Acceptance criteria include the following:

Design Basis

1 Verify that the range of operation of sensor (detector) channels ~~should be~~ is sufficient to cover the expected range of variation of the monitored variable during normal and transient (pulsing or square wave) reactor operation.

2 Verify that the RCS provides continuous indication of the neutron flux from subcritical source multiplication level through the licensed maximum power range. This continuous

indication should ensure about one decade of overlap in indication is maintained while observation is transferred from one detector channel to another.

3 Verify that the sensitivity of each sensor channel is commensurate with the precision and accuracy to which knowledge of the variable measured is required for the control of the reactor.

4 Verify that the system provides reliable reactor power level and rate-of-change information from detectors or sensors that directly monitor the neutron flux.

5 Verify that the system provides reliable information about the status and magnitude of process variables necessary for the full range of normal reactor operation.

6 Verify that the system is designed with sufficient control of reactivity for all required reactor operations including pulsing, and to ensure compliance with analyzed requirements on excess reactivity and shutdown margins.

7 Verify that the RCS provides redundant reactor power level indication through the licensed power range (i.e., redundant sensors with their own display).

8 Verify that the location and sensitivity of at least one reactor startup channel, along with the location and emission rate of the neutron startup source, is designed to ensure that changes in reactivity will be reliably indicated even with the reactor shut down (see Chapter 4).

9 Verify that a startup channel with interlock provides indication of neutrons and should prevent reactor startup (increase in reactivity) without sufficient neutrons in the core.

10 Verify that the startup and low-power range detectors is capable of discriminating against strong gamma radiation, such as that present after long periods of operation at full power, to ensure that changes in neutron flux density are reliably measured.

11 Verify that at least one neutron flux measuring channel provides reliable readings to a predetermined power level. For reactors with power as a safety limit, the measurable power level should be above the safety limit. For reactors without power as a safety limit, the measurable power level should be high enough to show that the basis for limiting licensed power level is not exceeded.

12 Verify that the automatic and manual control element absorber, drive, and display systems are designed to limit reactor periods and power oscillations and levels to values found acceptable in the reactor dynamic analyses in Chapter 4 of the SAR, and rod and driver positions should be clearly indicated for operator or interlock use.

13 Verify that the specifications on the I&C for the RCS are within the bounds of the normal range of environmental conditions.

14 Verify that the technical specifications, including surveillance tests and intervals, are based on SAR analyses and give the necessary confidence in availability and reliable operation of detection channels and control elements and devices.

Verify that the licensee has identified those I&C functions and variables to be probable subjects of technical specifications for the facility. The rate of change of reactivity of any unsecured experiment, any movable experiment, or any combination of such experiments introduced by intentionally setting the experiment(s) in motion relative to the reactor should not exceed the capacity of the control system to provide compensation.

15 If required by the SAR analysis, verify that the system provides a reactor period or a startup rate indication that covers subcritical neutron multiplication, the approach to critical, through critical, into the power range.

16 Verify that all interfaces between the RCS and RPS have been properly identified and addressed, thereby preserving the reliability, redundancy, and independence requirements of the RPS.

17 For reactors designed for pulsing or "square-wave" operation, verify that 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. Designs should be compared with such systems accepted by NRC for similar operations or reactors.

18 Verify that the control system includes the necessary features for manual and automatic control of process variables within prescribed normal operating limits. Functionality, which is included beyond the necessary minimum, should be reviewed to verify that unintended consequences of any added feature have been considered.

19 Verify that the control console and display system indicates the mode of operation, status, and change of status of the reactor control mode at all times for facilities with any automatic control modes.

Design Criteria

Independence

20 Verify any physical, electrical, and communications independence and isolation between safety system functions and the control system that are relied upon in the accident analysis to ensure execution of safety functions during and subsequent to any potential accident that requires a safety function. Verify that the RPS and ESF actuation system includes separation and isolation methods to protect them from any malfunctions or failures caused by other systems, including the RCS.

21 If independence is assumed in the accident analysis and a digital computer system used in a safety system is connected to a digital computer system used in a non-safety

system, verify that credible failures such as a logical or software malfunction of the non-safety system, would not affect the functions of the safety system.

Verify that the SAR considered credible failures of the RCS and the possible need for redundancy to protect the RPS and ESF actuation systems.

Fail Safe

22 Verify that the RCS is designed to assume a safe state on loss of electrical power (i.e., shutdown).

Effects of control system operation/failures

23 Verify that any mitigation of the Maximum Hypothetical Accident or potential accidents analyzed in Chapter 13 of the SAR do not rely on the operability of the reactor control system function to assure safety.

24 The RCS should not be designed to fail or operate in a mode that would prevent the RPS from performing its designed function, or prevent safe reactor shutdown. Verify that the failure of any control system component or any auxiliary supporting system for control systems is within the bounds of those facility conditions analyzed in Chapter 13 of the SAR. The reviewer should also verify that the safety analysis includes consideration of the effects of both control system action and inaction.

Operational Bypass

25 Verify that the applicant describes in the SAR interlocks to limit personnel hazards or prevent damage to systems during the full range of normal operations and any provisions for testing and bypassing are indicated in the control room.

26 Verify that experimental facilities or experiments that contain interlocks will not compromise the function of the RCS, or safe reactor shutdown will not be compromised.

Surveillance

27 The subsystems and equipment of the RCS should be readily tested and capable of being accurately calibrated. Verify that surveillance test and self-test features for a digital computer-based RCS address failure detection, self-test features (e.g., monitoring memory and memory reference integrity, using watch-dog timers or processors, monitoring communication channels, monitoring central processing unit status, and checking data integrity), and actions taken upon failure detection.

28 Verify that the description of the control elements, their drivers, and display or interlock components demonstrate that they

29 Verify that the applicant plans and describes how all control elements, their driver and release devices, and display or interlock components will be calibrated, inspected, and tested periodically to ensure operability as analyzed in the SAR.

Quality

30 The control systems should be designed and of sufficient quality to minimize the potential for challenges to safety systems. Verify that the quality of the components and modules in the RCS are commensurate with their safety importance.

31 Verify that the licensee's QA program provides controls over the design, fabrication, installation, and modification of the RPS and experimental equipment to the extent that these impact safety-related items. For RTRs, the licensee may use the guidance of ANSI/ANS 15.8-1995, as endorsed by RG 2.5, in developing a quality assurance program for complying with the program requirements of 10 CFR 50.34, subsections (a)(7) and (b)(6)(ii).

Use of Digital Systems

32 Verify that control system failures cannot have an adverse effect on safety system functions and will not pose frequent challenges to the safety systems. An area of special emphasis for control systems is to assure that the control system design is consistent with the commitments for control system/safety system independence. Isolation of safety systems from control system failures should be addressed.

Verify that applicants used a structured process in developing the control system software to minimize the potential for control system failures that could challenge safety systems. Perform a limited review of the functional requirements, the development process, the process implementation, and the design outputs of the control system software.

Access Control

33 Verify that the licensee has implemented measures throughout the software life-cycle to limit physical and electronic access to control system software and parameters to prevent changes by unauthorized personnel.

Cyber Security

34 Verify that the licensee has adequately addressed potential security vulnerabilities in each phase of the digital safety system lifecycle. The lifecycle phase-specific security requirements should be commensurate with the risk and magnitude of the harm resulting from unauthorized and inappropriate access, use, disclosure, disruption, or destruction of the digital safety system.

Review Procedures

This chapter of the SAR should describe the I&C subsystems that apply to all normal functions and parameters of the entire reactor facility; these subsystems constitute the RCS. The reviewer

should confirm that I&C information for all normal functions and systems described in other chapters of the SAR is addressed in this section.

The RCS comprises several subsystems; therefore, the reviewer should anticipate that the information in the SAR will be further subdivided, as noted in the section on the areas of review. The subdivisions should address all of the factors listed in Section 7.2 for each subsystem and should state how and where the subsystems interact and interface functions as a total RCS for normal operations. The reviewer should verify that all design bases are justified, and that the designs themselves accurately and completely implement the applicable bases and acceptance criteria. The reviewer should obtain the assistance of experts in the I&C Branch to review computer systems

Evaluation Findings

This section of the SAR should contain sufficient information to support the following types of conclusions, which will be included in the staff's safety evaluation report:

- The applicant has analyzed the normal operating characteristics of the reactor facility, including thermal steady-state power levels, pulsing capability (if included), and the planned reactor uses. The applicant has also analyzed the functions of the reactor control system (RCS) and components designed to permit and support normal reactor operations, and verifys that the RCS and its subsystems and components will give all necessary information to the operator or to automatic devices to maintain planned control for the full range of normal reactor operations. I The components and devices of the RCS are designed to sense all parameters necessary for facility operation with acceptable accuracy and reliability, to transmit the information with high accuracy in a timely fashion, and control devices are designed for compatibility with the analyzed dynamic characteristics of the reactor.

- The applicant has ensured sufficient interlocks, redundancy, and diversity of subsystems to avoid total loss of operating information and control, to limit hazards to personnel, and to ensure compatibility among operating subsystems and components in the event of single isolated malfunctions of equipment.

- The RCS was designed so that any single malfunction in its components, either analog or digital, would not prevent the reactor protection systems from performing necessary functions, or would not prevent safe shutdown of the reactor.

- Discussions of testing, checking, and calibration provisions, and the bases of technical specifications including surveillance tests and intervals give reasonable confidence that the RCS will function as designed.

The applicant has evaluated descriptions of planned interlocks or feedback controls from experimental apparatus to decrease postulated deleterious effects on the reactor. This review was coordinated with the effort for Chapters 10, "Experimental Facilities and Utilization," and 13, Accident Analyses," and with Section 7.4, 'Reactor Protection System." Furthermore, the design bases for such interlocks for future (not fully planned) experiments have been reviewed. The

designs and design bases of the RCS give reasonable assurance that experiments will be planned and accomplished with due regard for protection of the reactor.

7.4 Reactor Protection System

In this section, the applicant should thoroughly discuss and describe the RPS, listing the protective functions performed by the RPS, and the parameters monitored to detect the need for protective action. The principal action designed for the RPS 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, in order to prevent reactor operation in regions in which fuel damage events could occur. The automatic insertion may also be initiated manually by the operator. Parameters typically monitored for this purpose include core neutron flux, fuel temperature (primarily in TRIGA-designs), primary coolant flow and temperature, coolant level or radioactivity, and reactor area radiation levels. Redundant and diverse channels should normally monitor these parameters so that a single failure or malfunction cannot disable the protective function. As noted previously, unless analyses in the SAR require it, the RPS and the RCS need not be isolated and independent for non-power reactors. The objective of this review is to confirm that the RPS is designed to perform the safety functions stated in the SAR.

Areas of Review

In evaluating this system, the reviewer should include the following: sensors, signal handling equipment, isolation devices, bistable components, logic matrices, computer hardware and software, bypasses and interlocks associated with the trip and control circuitry, power supplies, and actuation devices that are designed to initiate automatic reactor shutdown or runback. The reviewer should examine how the RPS automatically initiates rapid operation of the reactivity control devices to verify that reactor design limits analyzed in the SAR are not exceeded. The SAR should contain the information recommended in the format and content guide, such as:

- Design bases, acceptance criteria, and guidelines used for design of the RPS.
- Descriptive information, including system logic and schematic diagrams, showing all instruments, computer hardware and software, electrical, and electromechanical equipment used in detecting reactor conditions requiring scram or other reactor protective action and in initiating the action.
- Analysis of adequacy of the design to perform the functions necessary to ensure reactor safety, and its conformance to the design bases, acceptance criteria, and the guidelines used.
- Assessment of the suitability of detector channels for initiating reactor protection (scrams). The reviewer should coordinate this effort with the review of other SAR sections.
- Proposed trip setpoints, time delays, accuracy requirements, and actuated equipment response to verify that the RPS is consistent with the SAR analyses of safety limits, limiting safety system settings (LSSS), and limiting conditions of operation (LCOs), and

that this information is adequately included in the technical specifications as discussed in Chapter 14, “Technical Specifications."

- Computer hardware, software, and software verification and validation programs for reactor designs that use computerized protection subsystems.

- Verification that surveillance tests and intervals give confidence that the equipment will reliably perform its safety function. Coordinate this effort with the review of the technical specifications.

- Consideration of the SAR analyses for the RPS to be designed to perform its safety function after a single failure and to meet requirements for seismic and environmental qualification, redundancy, diversity, and independence.

Acceptance Criteria

Most non-power reactors can be designed and operated with an acceptable small or insignificant radiological risk to the public or to the environment. The SAR should address the separation and independence of the RCS and the RPS with consideration of the radiological risk of reactor operation, because these systems include most of the same types of subsystems and components and similar functions. If the safety analysis in the SAR shows that safe reactor operation and safe shutdown would not be compromised by combination of the two systems, they need not be separate, independent, or isolated from each other. In practice, the reactor protection function for non-power reactors has been reliably accomplished by adding an automatic trip and rod release subsystem to the RCS or adding safety channels. Since many licensed non-power reactors have been designed on that principle, this section of the review guidance is based on its continuing applicability and acceptability.

The acceptance criteria for the RPS should include the following:

7.4 Reactor Protection System

In this section, the applicant should thoroughly discuss and describe the RPS, listing the protective functions performed by the RPS, and the parameters monitored to detect the need for protective action. The principal action designed for the RPS 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, in order to prevent reactor operation in regions in which fuel damage events could occur. The automatic insertion may also be initiated manually by the operator. Parameters typically monitored for this purpose include core neutron flux, fuel temperature (primarily in TRIGA-designs), primary coolant flow and temperature, coolant level or radioactivity, and reactor area radiation levels. Redundant and diverse channels should normally monitor these parameters so that a single failure or malfunction cannot disable the protective function. As noted previously, unless analyses in the SAR require it, the RPS and the RCS need not be isolated and independent for non-power reactors. The objective of this review is to confirm that the RPS is designed to perform the safety functions stated in the SAR.

Areas of Review

In evaluating this system, the reviewer should include the following: sensors, signal handling equipment, isolation devices, bistable components, logic matrices, computer hardware and software, bypasses and interlocks associated with the trip and control circuitry, power supplies, and actuation devices that are designed to initiate automatic reactor shutdown or runback. The reviewer should examine how the RPS automatically initiates rapid operation of the reactivity control devices to verify that reactor design limits analyzed in the SAR are not exceeded. The SAR should contain the information recommended in the format and content guide, such as:

- Design bases, acceptance criteria, and guidelines used for design of the RPS.
- Descriptive information, including system logic and schematic diagrams, showing all instruments, computer hardware and software, electrical, and electromechanical equipment used in detecting reactor conditions requiring scram or other reactor protective action and in initiating the action.
- Analysis of adequacy of the design to perform the functions necessary to ensure reactor safety, and its conformance to the design bases, acceptance criteria, and the guidelines used.
- Assessment of the suitability of detector channels for initiating reactor protection (scrams). The reviewer should coordinate this effort with the review of other SAR sections.
- Proposed trip setpoints, time delays, accuracy requirements, and actuated equipment response to verify that the RPS is consistent with the SAR analyses of safety limits, limiting safety system settings (LSSS), and limiting conditions of operation (LCOs), and that this information is adequately included in the technical specifications as discussed in Chapter 14, “Technical Specifications."
- Computer hardware, software, and software verification and validation programs for reactor designs that use computerized protection subsystems.
- Verification that surveillance tests and intervals give confidence that the equipment will reliably perform its safety function. Coordinate this effort with the review of the technical specifications.
- Consideration of the SAR analyses for the RPS to be designed to perform its safety function after a single failure and to meet requirements for seismic and environmental qualification, redundancy, diversity, and independence.

Acceptance Criteria

Most non-power reactors can be designed and operated with an acceptable small or insignificant radiological risk to the public or to the environment. The SAR should address the separation and independence of the RCS and the RPS with consideration of the radiological risk of reactor operation, because these systems include most of the same types of subsystems and components and similar functions. If the safety analysis in the SAR shows that safe reactor operation and safe shutdown would not be compromised by combination of the two systems,

they need not be separate, independent, or isolated from each other. In practice, the reactor protection function for non-power reactors has been reliably accomplished by adding an automatic trip and rod release subsystem to the RCS or adding safety channels. Since many licensed non-power reactors have been designed on that principle, this section of the review guidance is based on its continuing applicability and acceptability.

The acceptance criteria for the RPS should include the following:

Design Basis

1 Verify that the reactor has operable protection capability in all operating modes and conditions, as analyzed in the SAR. For example, at low reactor power, a reactor period scram may be needed to ensure that inadvertent transients could not propagate risks to personnel or the reactor.

2 Verify that the range of operation of sensor (detector) channels is sufficient to cover the expected range of variation of the monitored variable during normal and transient (pulsing or square wave) reactor operation.

3 Verify that information about the RPS detector or sensor devices is 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.

4 Verify that the system requirements (such as required scram times) are clearly identified and are consistent with the system requirements in the accident analyses and technical specifications (Sections 13 and 14).

5 Verify that the automatic reactor runback or shutdown (scram) subsystem is fail-safe against malfunction and electrical power failure should be as close to passive as can be reasonably achieved, should go to completion once initiated, and should go to completion within the time scale derived from applicable analyses in the SAR.

6 Verify that the scram system is designed to maintain reactor shutdown without operator action to at least the shutdown margin as defined in Chapter 4 and the technical specifications.

7 Verify, if applicable, that the count rate interlock functions properly in a high gamma field and that all reactivity changes can be properly monitored until the startup channel indication overlaps the log or linear channel power indication.

8 Verify that those variables with a spatial dependency that the minimum number and location of sensors are identified and shown to be adequate for the safety purposes.

9 Verify that no single failure can cause the failure of more than one redundant sensing line unless it can be demonstrated that the protective function is still accomplished.

10 Verify that the design properly documents the permissive conditions for each operating bypass capability that is to be provided.

11 Verify that the RPS is designed for reliable operation in the normal range of environmental conditions anticipated within the facility.

12 Verify that system timing requirements calculated from the maximum hypothetical accidents and other criteria have been allocated to the digital computer portion of the system as appropriate, and have been satisfied in the digital system architectural design. In addition, verify that the installed systems perform as predicted and appropriate measurement and analysis techniques have been used to compensate for the uncertainties introduced by certain design and implementation practices, such as the use of interrupts.

13 Verify that the RPS function and time scale can be readily tested to ensure operability of at least minimum protection for all reactor operations.

Design Criteria

Single Failure

14 Each scram channel has a separate set of contacts or other bi-stable component to trip the RPS system. Verify that redundant detector channels and control elements provide assurance that a single random failure or malfunction in the RCS or RPS, or from any other system, could not prevent the RPS from performing its intended function, or prevent safe reactor shutdown.

15 Verify that the RPS incorporates multiple means for responding to each event discussed in the SAR Chapter 13. At least one pair of these means for each event should have the property of signal diversity (i.e., the use of different sensed parameters to initiate protective action, in which any of the parameters may independently indicate an abnormal condition, even if the other parameters are sensed incorrectly).

Independence

16 Verify that the appropriate logic, schematic, and circuit diagrams are included and should show independence of detector channels and trip circuits.

17 Verify that physical separation and electrical isolation are used to maintain the independence of RPS circuits and equipment among redundant safety divisions or with non-safety systems so that the safety functions required during and following any maximum hypothetical accident can be accomplished.

18 Verify that any communications—within a single safety channel, between safety channels, and between safety and nonsafety computers—does not adversely affect the performance of required safety functions.

19 Verify that the protocol selected for the data communications meet the performance requirements of all supported systems. This review should also include verification that data communications for the RPS system timing is deterministic or bounded.

Verify the protocol implementations conform to validated protocol specifications by formally generated test procedures and test data vectors and that the implementations themselves were constructed using a formal design process that ensures consistency between the product and the validated specification.

Verify that no unexpected performance deficits exist that could adversely affect the proposed RPS architecture.

Equipment Qualification

20 Verify that the licensee has shown that the specifications on the I&C are within the bounds of the normal range of environmental conditions.

21 Verify that the effects of EMI/RFI and power surges on safety-related I&C systems, including computer-based digital systems are adequately addressed.

Prioritization of functions

22 Verify that devices that receive signals from safety and non-safety sources prioritize the signal the safety system.

Setpoints

23 Verify that the setpoints for an actuation of the RPS are based on a documented analysis methodology that identifies assumptions and accounts for uncertainties, such as environmental allowances and measurement / computational errors associated with each element of the instrument channel. The analysis parameters and assumptions should be consistent with the safety analysis, system design basis, technical specifications, facility's design, and expected maintenance practices.

24 Verify that an adequate margin exists between setpoints and safety limits, such that the system initiates protective actions before safety limits are exceeded.

25 Verify that the sensitivity of each sensor channel is commensurate with the precision and accuracy to which knowledge of the variable measured is required for the protective function.

26 Verify that administrative controls or automatic means are provided for changing setpoints when the operating mode of the reactor is changed.

Operational Bypass/Permissives and Interlocks

27 Verify that appropriate controls are provided for interlock initiation and bypass.

28 Verify that the ability to initiate any bypass or deliberately induced inoperability of a safety function and of the systems actuated or controlled by the safety function during operation are immediately announced both audibly and visually. Thereafter, continuous

indication of each active bypass should be provided in the normal and immediate field of vision of the reactor operator.

Verify that provisions exist to allow the operations staff to confirm that a bypassed safety function has been properly returned to service.

29 Verify that the capability of a safety system to accomplish its safety function should be retained while execute features equipment is in maintenance bypass. Portions of the execute features with a degree of redundancy of one should be designed such that when a portion is placed in maintenance bypass (that is, reducing temporarily its degree of redundancy to zero, the remaining portions provide acceptable reliability.

30 If the safety analysis shows that the RPS/RCS should be separate systems, verify that the licensee has shown that there are barriers isolating the RPS and RCS systems or that the combined system is a safety-related system. Any isolation devices should assure that credible failures in the connected non-safety or redundant channels will not prevent the safety systems from meeting their required functions.

Surveillance

31 The RPS should be sufficiently distinct in function from the RCS that its unique safety features can be readily tested, verified, and calibrated. Verify that the RPS is designed to allow testing, calibration, and inspection.

32 Verify that the testing, calibration, and inspections of the RPS are sufficient to show that once performed confirms the operability of the RPS. Verification should include confirming that surveillance test and self-test features for a digital computer-based RPS address failure detection, self-test features (e.g., monitoring memory and memory reference integrity, using watch-dog timers or processors, monitoring communication channels, monitoring central processing unit status, and checking data integrity), and actions taken upon failure detection.

33 Technical specifications, including surveillance tests and intervals, should be based on discussions and analyses in the SAR of required safety functions. Verify that the proposed design and the justification for test intervals are consistent with the surveillance testing proposed as part of the facility technical specifications.

Verify that the licensee has identified those I&C functions and variables to be probable subjects of technical specifications for the facility. The rate of change of reactivity of any unsecured experiment, any movable experiment, or any combination of such experiments introduced by intentionally setting the experiment(s) in motion relative to the reactor should not exceed the capacity of the control system to provide compensation.

Classification and Identification

34 Verify that the RPS equipment is distinctly identified to indicate its safety classification and to associate equipment according to divisional or channel assignments.

Human Factors

35 Verify that human factors were considered at the initial stages and throughout the design process to assure that the functions allocated in whole or in part to the operator(s) can be successfully accomplished to meet the safety system design goals.

36 Verify that the scram operator is able to operate the system by means of readily available switches, or by interlock activation.

37 Verify that the scram system is designed to annunciate the channel initiating the action, and to require resetting to resume operation.

Quality

38 Verify that the quality of the components and modules in the RPS are commensurate with their safety importance.

39 Verify that the licensee's QA program provides controls over the design, fabrication, installation, and modification of the RPS and experimental equipment to the extent that these impact safety-related items. For RTRs, the licensee may use the guidance of ANSI/ANS 15.8-1995, as endorsed by RG 2.5, in developing a quality assurance program for complying with the program requirements of 10 CFR 50.34, subsections (a)(7) and (b)(6)(ii).

Use of Digital Systems

40 Verify that the development of the digital safety system followed a formally defined life-cycle process and that potential security vulnerabilities in each phase of the digital safety system lifecycle were addressed. The lifecycle phase-specific security requirements should be commensurate with the risk and magnitude of the harm resulting from unauthorized and inappropriate access, use, disclosure, disruption, or destruction of the digital safety system.

41 Verify that the tasks for validating and verifying that the software development activities have been carried out in their entirety. Documentation should exist that shows that the V&V tasks have been successfully accomplished for each life cycle activity group.

42 Verify that the configuration management program appropriately traces software changes—from their point of origin to implementation, and addresses any impacts on system safety.

43 Verify that the safety analysis activities have been successfully accomplished for each life cycle activity group. In particular, verify that the system safety requirements have been adequately addressed for each activity group; that no new hazards have been introduced; that the software requirements, design elements, and code elements that can affect safety have been identified; and that all other software requirements, design, and code elements will not adversely affect safety.

44 Verify the computer system qualification testing tests all portions of the computer necessary to accomplish its safety functions, and that those portions whose operation or failure could impair safety functions, were also exercised during testing.

45 Verify that the functional characteristics for the software requirements specifications are properly (and precisely) described for each requirement.

46 When reliability goals are identified, verify that the proof of meeting the goals include the software.

Access Control

47 Verify that the design or administrative controls prevent/limit unauthorized access to safety system equipment and software. Administrative controls can be supported by provisions within the safety systems, by provision in the RTR design, or by a combination thereof.

48 To provide assurance that the required computer system hardware and software are installed in the appropriate system configuration, verify that the licensee has a program to ensure that the correct version of the software/firmware is installed in the correct hardware components.

Cyber Security

49 Verify that the licensee has adequately addressed potential security vulnerabilities in each phase of the digital safety system lifecycle. The lifecycle phase-specific security requirements should be commensurate with the risk and magnitude of the harm resulting from unauthorized and inappropriate access, use, disclosure, disruption, or destruction of the digital safety system.

Review Procedures

The reviewer should compare the design bases for the RPS with SAR analyses of possible hazards to the reactor or to personnel that could be prevented or mitigated by timely protective action. The RPS design and planned functional operation should be compared with the design bases and with the acceptance criteria for this section. The review should be sufficiently detailed to allow assessment of the complexity of the RPS and evaluation of opportunities for malfunction or operability failure during reactor operation. The reviewer should compare the RPS logic and design features with acceptable systems on similar reactors whose operating history is available. The reviewer should obtain the assistance of experts in the I&C Branch to review computer systems.

Evaluation Findings

This section of the SAR should contain sufficient information to support the following types of conclusions, which will be included in the staffs safety evaluation report:

- The applicant has analyzed the design and operating principle of the reactor protection system (RPS) for the (insert name of facility). The protection channels and protective responses are sufficient to ensure that no safety limit, limiting safety system setting, or RPS-related limiting condition of operation discussed and analyzed in the SAR will 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 normal operations poses no undue radiological risk to the health and safety of the public, the facility staff, or the environment.

7.5 Engineered Safety Features Actuation Systems

Non-power reactors can generally be designed and operated so they pose an acceptably small or insignificant radiological risk to the public. If the SAR analyses show that no unacceptable radiation doses would result from any postulated accident, even without consequence mitigation, such a facility need not include ESFs. The reviewer should, therefore, study Chapter 6, “Engineered Safety Features," and Chapter 13 of the SAR to determine if there is a requirement for ESFs and their related ESF actuation system. The guidance in this section applies to any non-power reactor for which an ESF is required.

Areas of Review

The reviewer should evaluate the information in Chapter 6 describing the ESFs, the scenarios of the postulated accidents in Chapter 13 which involve the use of an ESF, and the detector channels that sense the need for mitigation of possible consequences. The information to be reviewed in this section should also include the design criteria of each ESF actuation system, and the design bases and functional requirements for the ESF actuation systems. Additional information for review should include details of the design and operating characteristics of the actuation systems such as the following:

The review of the ESF actuation systems should include the bases, criteria, standards, and guidelines used for the design of the ESF actuation systems, including the basis for evaluating the reliability and performance of the I&C systems.

The review of the ESF actuation systems should include a description, including logic, schematics, and functional diagrams, of the overall system and component subsystems.

A system description with diagrams and auxiliary information should be sufficiently complete to allow a thorough review of all aspects of the ESF actuation systems including normal/abnormal operation, maintenance, and accident scenarios. The description should include the description of instruments, computer hardware and software, electromechanical components, detector channels, trip devices and set points.

The review of the ESF actuation systems should include the following:

- analysis of the adequacy of the design to establish conformance to the design bases and criteria for reactor power, rate of power change, and pulsing information;
- analysis of the adequacy of the design to establish conformance to the design bases and criteria for information on required process variables to control reactor operation;
- application of the functional design and analyses to the development of bases of technical specifications, including surveillance tests and intervals; and
- ESF actuation systems failure modes to determine if any malfunction of the ESF actuation systems could prevent the RPS from performing its safety function, or could prevent safe shutdown of the reactor.

Acceptance Criteria

The acceptance criteria together with the use of good engineering practice will help the reviewer to conclude whether the ESF actuation systems are designed to provide for the reliable control of reactor power level, rate of change of power levels, and pulsing (if applicable) during reactor startup, the full range of normal operation, and shutdown. Acceptance criteria include the following:

Design Basis

1 Verify that the ESF actuation systems are designed to be operable whenever an accident could happen for which the SAR shows consequence mitigation is necessary.

2 Verify that the range and sensitivity of ESF actuation system sensors are sufficient to ensure timely and accurate signals to the actuation devices.

3 Verify that the provisions for manual control have been identified and minimum criteria for each manual action are specified.

4 Verify that the ESF inputs are derived from signals that are direct measures of the desired variables as specified in the design basis or that the indirect parameters are a valid representation of the desired parameters.

5 Verify that those variables with a spatial dependency that the minimum number and location of sensors are identified and shown to be adequate for the safety purposes.

6 Verify that the design properly documents the permissive conditions for each operating bypass capability that is to be provided.

7 Verify that the equipment is designed to operate reliably in the ambient environment until the accident has been brought to a stable condition. The environment qualification should also include confirmation that the instrument sensing lines were included in the licensees design.

8 Verify that any auxiliary features that are part of the ESF actuation systems by association do not inhibit the performance of the safety function of the ESF actuation systems.

9 Verify that the system timing requirements calculated from design basis accidents and other criteria are appropriately allocated to the digital computer portion of the ESF actuation systems and be satisfied in the digital system architectural design. The real-time performance of the ESF actuation systems should include verification that system timing is deterministic or bounded. Time delays within the digital ESF actuation systems and measurement inaccuracies introduced by the digital components should be accounted for in the establishment of the instrumentation setpoints. Timing should be accounted for in system response and verified in testing. Practices should address asynchronous operation of separate modules.

Design Criteria

Single Failure

10 Verify that the ESF actuation system is designed not to fail or operate in a mode that would prevent the RPS from performing its designed function, or prevent safe reactor shutdown.

11 Verify that the ESF actuation systems I&C system is designed to perform its protective function after experiencing a single random active failure within the system. For digital computer-based ESF actuation systems, the applicant/licensee should have performed a defense-in-depth and diversity analysis.

Independence

12 Verify that any interconnections among safety divisions for an RPS/ESF actuation system or between an RPS/ESF actuation systems channel and non-safety components/systems do not prevent those safety functions required during and following any design basis accident from accomplishing its mission.

13 Verify the independence of the ESF actuation systems to ensure that the safety functions required during and following any design basis accident can be accomplished.

Equipment Qualification

14 Verify that the effects of EMI/RFI and power surges on safety-related I&C systems, including computer-based digital systems are adequately addressed.

Fail Safe

15 Verify that the ESF actuation system is designed to assume a safe state on loss of electrical power.

Setpoints

16 Verify that the setpoints for an ESF actuation are based on a documented analysis methodology that identifies assumptions and accounts for uncertainties, such as environmental allowances and measurement / computational errors associated with each element of the instrument channel. The analysis parameters and assumptions should be consistent with the safety analysis, system design basis, technical specifications, facility design, and expected maintenance practices.

17 Where it is necessary to provide multiple setpoints for adequate protection based on particular modes of operation or sets of operating conditions, verify that the ESF actuation systems provides positive means of ensuring that the more restrictive setpoint is used when required.

Operational Bypass/Permissives and Interlocks

18 Verify that the ESF actuation systems design provides an operating bypass capability only where necessary to accommodate essential function such as changes in operating mode of the reactor or periodic operational testing. Provisions should exist to prevent activation of an operating bypass unless applicable permissive conditions exist. No bypass capability should be provided for the mechanisms to manually initiate ESF actuation systems actions.

19 If provisions for maintenance or operating bypasses are provided, verify that the ESF actuation systems design retains the capability to accomplish its safety function while a bypass is in effect.

20 Verify that the ESF actuation systems design provides an indication system to announce the initiation of any bypass during operation and to continuously indicate the bypass status of ESF actuation systems components.

Completion of Protective Actions

21 Verify that the ESF actuation systems design ensures that the safety actions will continue until the mitigation function is completed. Only deliberate operator action should be permitted to reset the ESF actuation systems or its components. The mechanisms for deliberate operator intervention in ESF actuation systems status or its functions should not be capable of preventing the initiation of ESF actuation systems actions.

Surveillance

22 Verify that the equipment in the ESF actuation systems I&C system (from sensors to actuated devices) are designed to be readily tested and calibrated to ensure operability.

23 Verify that the testing, calibration, and inspections of the RPS are sufficient to show that once performed confirms the operability of the RPS. Verification should include confirming that surveillance test and self-test features for a digital computer-based RPS address failure detection, self-test features (e.g., monitoring memory and memory reference integrity, using watch-dog timers or processors, monitoring communication channels, monitoring central processing unit status, and checking data integrity), and actions taken upon failure detection.

24 Verify that technical specifications including surveillance tests and intervals ~~should~~ ensure availability and operability of the ESF actuation system.

25 Where safety system testing during operation is required or provided as an option, verify that the ESF actuation systems design retains the capability to accomplish its safety function while under test.

Classification and Identification

26 Verify that the ESF actuation systems equipment is distinctly identified to indicate its safety classification and to associate equipment according to divisional or channel assignments.

Human Factors

27 Verify that human factors were considered at the initial stages and throughout the design process to assure that the functions allocated in whole or in part to the operator(s) can be successfully accomplished to meet the safety system design goals.

Quality

28 Verify that the engineering design of ESF actuation systems and the components procured for them are of high quality to ensure reliable operation.

29 Verify that the quality assurance program provides controls over the design, fabrication, installation, and modification of the ESF actuation systems and experimental equipment to the extent that these impact safety-related items.

Use of Digital Systems

30 Verify that for each design basis accident for which an ESF actuation systems is required the frequency of its failure is low (two or more independent failures required) or the consequences of its failure pose more than an acceptably small radiological risk.

31 Verify that the development of the digital safety system followed a formally defined life-cycle process and that potential security vulnerabilities in each phase of the digital safety system lifecycle were addressed. The lifecycle phase-specific security requirements should be commensurate with the risk and magnitude of the harm resulting from unauthorized and inappropriate access, use, disclosure, disruption, or destruction of the digital safety system.

32 When reliability goals are identified, verify that the proof of meeting the goals include the software.

Access Control

33 Verify that the design or administrative controls prevent/limit unauthorized access to safety system equipment and software. Administrative controls can be supported by provisions within the safety systems, by provision in the RTR design, or by a combination thereof.

Cyber Security

34 Verify that the licensee has adequately addressed potential security vulnerabilities in each phase of the digital safety system lifecycle. The lifecycle phase-specific security requirements should be commensurate with the risk and magnitude of the harm resulting from unauthorized and inappropriate access, use, disclosure, disruption, or destruction of the digital safety system.

Review Procedures

The reviewer should compare the design criteria and bases of the ESF actuations system with the designs of the ESFs and the accident scenarios and possible consequences. The reviewer should also compare the design and functional descriptions of the ESF actuation system with the acceptance criteria and with applicable criteria and functions discussed in Chapters 6 and '13. The reviewer should obtain the assistance of experts in the I&C Branch to review computer Systems.

Evaluation Findings

This section of the SAR should contain sufficient information to support the following types of conclusions, which will be included in the staff's safety evaluation report:

- The applicant has analyzed the scenarios for all postulated accidents at the facility, including all accidents for which consequence mitigation by engineered safety features (ESFs) is required or planned. The staff evaluated the ESFs and has determined that the designs of their actuation systems give reasonable assurance of reliable operation if required.

- The applicant has considered the environments in which the ESFs are expected to operate, and the applicable actuation systems have been designed accordingly to function as required.

- The design considerations of the ESF actuation system give reasonable assurance that the system will detect changes in measured parameters as designed and will initiate timely actuation of the applicable ESF.

- The bases for technical specifications, including surveillance tests and intervals for the ESF actuating system, give reasonable assurance of actuation of ESFs when required.

7.6 Control Console and Display Instruments

Areas of Review

The non-power reactor control room, containing the control console and other status display instruments is the hub for reactor facility operation. It is the location to which all information necessary and sufficient for safe and effective operation of the facility is transmitted, and the primary location from which control and safety devices are actuated either manually or automatically. The console contains most of the circuitry and hardware for organizing and processing the information either analytically or digitally, applying decision logic, and routing signals to display devices or automatic action of other subsystems or both. The reviewer should evaluate the control console and display instruments to determine that the following are included:

- signals from instrument systems monitoring the reactor and other system process variables

- analytically or digitally processed outputs based on monitored variables

- indication of RCS or RPS status

- recording of selected variables and operating data

- annunciators and alarms

- personnel and equipment protection interlock status

- inputs to the RCS or RPS

- analog or computer hardware and software that manages the combination and presentation of reactor and process variable information for the operators

The review of the Control Console and Display Instruments should evaluate the design and location of the displays and operator control systems in the performance of operations necessary for the safe control of the reactor. Information supplied for review should include the following: (1) design criteria, bases, and guidelines used to design the control console and information display system; and (2) descriptive information such as logic, functional control and schematic diagrams, and equipment location drawings showing interrelationships in the control console.

The control console instruments and display systems should be designed to work with applicable systems, either analog or digital computers.

An objective of this review is to evaluate whether displays and operator control systems are designed and located to promote case and efficiency in the performance of operations necessary for the safe control of the reactor. The information should include the following:

- design criteria, bases, and guidelines used to design the control console and information display system
- descriptive information such as logic, functional control and schematic diagrams, and equipment location drawings showing interrelationships in the control console
- analysis of the adequacy of the design to perform the necessary, control and protection actuation, and information management, storage, and display functions
- coordination with review of other SAR chapters to verify control inputs and displayed parameters apply for the systems involved
- coordination with technical specifications review to verify that appropriate surveillance tests and intervals are specified to ensure that the instruments and equipment will perform their functions as designed

Acceptance Criteria

Acceptance criteria for the control console and display instruments should be based on good engineering practice and should include the following considerations:

Design Basis

1 Verify that the designed range of operation of each device is should be sufficient for the expected range of variation of monitored variables under conditions of operation.

2 Verify that the provisions for manual control have been identified and minimum criteria for each manual action are specified.

3 Verify that the control console and display equipment is designed to operate reliably in the ambient environment until the accident has been brought to a stable condition.

4 Verify that control, safety, and transient rod position indication and limit lights are displayed on the console and readily accessible and understandable to the reactor operator.

5 Verify that other controls and displays of important parameters that the operator should monitor to keep parameters within a limiting value, and those which can affect the reactivity of the core are readily accessible and understandable to the reactor operator.

6 Verify that the displays and controls provided for manual system-level actuation and control of safety equipment should be functional under conditions which may require manual actions.

7 Verify that a control console instrument system failure should not prevent the RPS from performing its safety function and should not prevent safe reactor shutdown.

8 Verify that any remote shutdown stations or monitors are secure and that their failure does not prevent safe reactor shutdown.

9 Verify that those manual controls that are connected to safety equipment are connected downstream of digital I&C safety system outputs (i.e., as close to the actuation device without any intervening logic).

10 Verify that the functional characteristics of the display and control digital components are sufficient to provide operators with the information needed to place and maintain a facility in a shutdown condition.

Design Criteria

Independence

11 Verify that operator workstations or displays that are associated with both safety and nonsafety functions do not impede execution of the safety function.

12 Verify that when required by the safety analysis, the control console instruments and equipment are designed to assume a safe state on loss of electrical power or should have a reliable source of emergency power sufficient to sustain operation of specific devices.

Prioritization of functions

13 If the design of the control console and display system includes multidivisional control and display stations, the use of operator workstations or displays that are associated with multiple safety divisions and/or with both safety and non-safety functions, verify that devices that receive signals from safety and non-safety sources prioritize the signal from the safety system.

Surveillance

14-15 Verify that the control console, display instruments, and equipment are ~~should be~~ readily testable and capable of being accurately calibrated.

Verify that the testing, calibration, and inspections of the control console, display instruments, and equipment are sufficient to show that once performed confirms the operability of the RPS. Verification should include confirming that surveillance test and self-test features

for a digital computer-based RPS address failure detection, self-test features (e.g., monitoring memory and memory reference integrity, using watch-dog timers or processors, monitoring communication channels, monitoring central processing unit status, and checking data integrity), and actions taken upon failure detection.

16 The bases for technical specifications, including surveillance tests and intervals for control console devices, should be discussed in this section of the SAR.

Verify that the proposed design and the justification for test intervals are consistent with the surveillance testing proposed as part of the facility technical specifications.

Human Factors

17 Verify that human factors were considered at the initial stages and throughout the design process to assure that the outputs and display devices showing reactor nuclear status are ~~should be~~ readily observable by the operator while positioned at the reactor control and manual protection systems.

Annunciators

18 Verify that annunciators or alarms should clearly show the status of systems such as operating systems, interlocks, experiment installations, pneumatic rabbit insertions, ESF initiation, radiation fields and concentration, and confinement or containment status.

19 Verify that hardware and software failures were evaluated in assessing the reliability of annunciators used to support normal and emergency operations.

20 For negligible risk research reactors that do not meet the single-failure criterion for the RPS, verify that the alarms alerting the operators of a failure are reliable, do not introduce a credible common failure mode, and appropriate administrative controls specify actions to be taken under such circumstances.

21 Verify that the system/channel surveillance tests include the annunciators and displays and that the tests satisfy the technical specification requirements.

22 Verify that those alarms for which no automatic control is provided meet same the requirements of the control console, display instruments, and equipment.

Quality

23 Verify that the quality of the control console, display instruments, and equipment are commensurate with their safety importance.

Use of Digital Systems

24 Verify that the configuration management program appropriately traces software changes—from their point of origin to implementation, and addresses any impacts on system safety for the control console, display instruments, and equipment.

25 To provide assurance that the required computer system hardware and software are installed in the appropriate system configuration, verify that the licensee has a program to ensure that the correct version of the software/firmware is installed in the correct hardware components.

26 Verify the computer system qualification testing tests all portions of the computer necessary to accomplish its safety functions, and that those portions whose operation or failure could impair safety functions, were also exercised during testing.

27 When reliability goals are identified, verify that the proof of meeting the goals include the software.

Access Control

28 Reactor operation should be prevented and not authorized without use of a key or combination input at the control console.

Verify that the design or administrative controls prevent/limit unauthorized access to safety system equipment and software. Administrative controls can be supported by provisions within the safety systems, by provision in the RTR design, or by a combination thereof.

Cyber Security

29 Verify that the licensee has adequately addressed potential security vulnerabilities in each phase of the digital safety system lifecycle. The lifecycle phase-specific security requirements should be commensurate with the risk and magnitude of the harm resulting from unauthorized and inappropriate access, use, disclosure, disruption, or destruction of the digital safety system.

Review Procedures

The reviewer should coordinate the review of this section with all other applicable chapters of the SAR because the control console and other display instruments in the reactor control room could be linked to numerous systems and subsystems in the reactor facility. The reviewer should compare the design bases and functional requirements of other reactor systems with those for the control console equipment. The reviewer should also compare the design of the console system with the acceptance criteria. The reviewer should study the arrangement of parameter displays, control devices, and the planned operator station to determine whether the operator can quickly understand information and take proper action. The reviewer should obtain the assistance of experts in the I&C Branch to review computer systems. The reviewer should note the discussion in the format and content guide about digital operator information display systems or operator aids.

Evaluation Findings

This section of the SAR should contain sufficient information to support the following types of conclusions, which will be included in the staffs safety evaluation report:

- The applicant has shown that all nuclear and process parameters important to safe and effective operation of the (insert name of facility) non-power reactor will be displayed at the control console. The display devices for these parameters are easily understood and readily observable by an operator positioned at the reactor controls. The control console design and operator interface are sufficient to promote safe reactor operation.

- The output instruments and the controls in the control console have been designed to provide for checking operability, inserting test signals, performing calibrations, and verifying trip settings. The availability and use of these features will ensure that the console devices and subsystems will operate as designed.
- The annunciator and alarm panels on the control console give assurance of the operability of systems important to adequate and safe reactor operation, even if the console does not include a parameter display

- The locking system on the control console reasonably ensures that the reactor facility will not be operated by unauthorized personnel.

7.7 Radiation Monitoring Systems

Areas of Review

In this section of the SAR, the applicant should address all equipment, devices, and systems used for monitoring or measuring radiation intensities or radioactivity, except for nuclear instruments. Information in this section should be reviewed in close coordination with those sections of Chapter 11, “Radiation Protection Program and Waste Management,” that discuss the use of radiation-monitoring systems to assess, evaluate, or control personnel or environmental radiological exposures. Chapter 11 should include sufficient information about the radiation monitoring systems to support confident use of the exposure and dose results and this section should detail the operating principles, designs, and functional performance of the I&C aspects of the system. Radiation measurements at a reactor facility may also be used for reactor diagnostic or safety purposes and the applicable equipment should be discussed in this section. Examples of such functions may include reactor coolant level, coolant radioactivity, fuel inventory measurements for self-protection, confinement or containment initiation, and experimental measurements.

The review of the Radiation Monitoring Systems should include the bases, criteria, standards, and guidelines used for the design of the Radiation Monitoring Systems.

For the Radiation Monitoring Systems, a discussion of the criteria for developing the design bases for the Radiation Monitoring Systems I&C system, including the basis for evaluating the reliability and performance of the I&C systems should be provided.

The review of the Radiation Monitoring Systems should include a description, including logic, schematics, and functional diagrams, of the overall system and component subsystems

A system description with diagrams and auxiliary information should be sufficiently complete to allow a thorough review of all aspects of the Radiation Monitoring Systems including normal/abnormal operation, maintenance, and accident scenarios.

The reviewer should evaluate radiation detectors and sampling equipment; signal processing equipment; computer hardware and software that controls sampling, detection, signal processing and logic; power supplies; and actuation systems that accomplish a function for the system. In determining if the I&C systems are designed to accomplish the radiation measurement functions, the reviewer should evaluate the following:

- analysis of the adequacy of the design to perform the stated function or purpose of the systems and conformance to the design bases, criteria, and guidelines used
- proposed trip, annunciation, or alarm setpoints, time delays, accuracy requirements, and actuated equipment response to verify that they are consistent with applicable analyses and limiting conditions for operation in the SAR
- coordination with review of other applicable SAR chapters to assess the suitability of the monitored parameters for accomplishing the purposes
- coordination with applicable technical specifications review to verify that surveillance tests and intervals are specified to give confidence that the system and equipment will be operable and reliably perform its function
- consideration of the need for single failure protection, seismic and environmental qualification protection, and diversity.

Acceptance Criteria

Acceptance criteria for radiation monitoring systems should include the following:

Design Bases

1 Verify that the instrument ranges are ~~should be~~ sufficient to cover the expected range of variation of the monitored variable under the full range of normal operation and, if assumed in the SAR analysis, accident conditions. If two or more instruments are needed to cover a particular range, overlapping of instrument span is provided. If the required range of monitoring instrumentation results in a loss of instrumentation sensitivity in the normal operating range, separate instruments are used.

2 If the radiation monitoring systems provide input to the RPS or ESF actuation systems, verify that it meets the applicable criteria and requirements in Sections 7.4 and 7.5 for those systems.

3 Verify that the applicant properly developed and maintains the display criteria documentation for the accident monitoring variables.

4 Verify that the radiation monitoring systems are designed to interface with either analog or digital computerized RCS or RPS if applicable.

5 Verify that the systems and equipment in the radiation monitoring systems are designed for reliable operation in the environment in which they will function.

6 Verify that the sensitivity and accuracy of each system is commensurate with the precision and accuracy to which knowledge of the variable is required by analysis or design basis.

7 Verify that the time delays, including sensor response time, signal processing delay and update frequency of the accident monitoring instrumentation are consistent with applicable analyses and limiting conditions for operation described in Chapter 13 of the SAR.

Design Criteria

Single Failure

8 Verify that the radiation monitoring systems are designed not to fail or operate in a mode that would prevent the RPS from performing its safety function, or prevent safe reactor shutdown. The review of computer-based digital systems should consider the unique aspects of digital I&C including new or unique failure modes specific to digital I&C systems.

9 Verify that no single failure within the accident-monitoring instrumentation, its auxiliary supporting features, or its power sources concurrent with failures that are a result of a specific accident (excluding external events, such as fire) should prevent operators from being presented information necessary for them to determine safety status of the facility and to bring the facility to and maintain it in a safe condition following that accident. The reviewer should also evaluate the need for diversity.

Independence

10 Verify that any communications—within a single safety channel, between safety channels, and between safety and nonsafety computers—does not adversely affect the performance of required safety functions.

Surveillance

11-12 Verify that the systems and equipment are designed for easy testing and capable of accurate calibration. The I&C systems should be designed to accomplish the radiation measurement functions. The review should verify that surveillance tests and intervals are specified to give confidence that the system and equipment will be operable and reliably perform its function.

If the digital equipment in the radiation monitoring systems include self-diagnostic capabilities to aid in troubleshooting, verify that that the testing, calibration, and

inspections are sufficient to show that once performed confirms the operability of the radiation monitoring system. Verification should include confirming that surveillance test and self-test features for a digital computer-based systems address failure detection, self-test features (e.g., monitoring memory and memory reference integrity, using watch-dog timers or processors, monitoring communication channels, monitoring central processing unit status, and checking data integrity), and actions taken upon failure detection.

13 Verify that the bases of the technical specifications, including surveillance tests and intervals, are sufficient to ensure that the systems will be operable and will perform their designed functions.

Human Factors

14 Verify that the selection, type, location, and display of radiation monitoring system variables were determined considering human factors analyses.

Display and Recording

15 Verify that the display characteristics for accident monitoring variables were established based on results of an analysis of the system functions required for accident response and the operator-executed tasks required for those functions during design basis accidents.

16 Verify that those accident monitoring variables associated with fuel failures or breach of a fission product barrier are uniquely identified with a characteristic designation so that the operator can easily discern information intended for use under accident conditions.

17 Verify that variables monitored used in determining and continuously assessing the magnitude of radioactive material release.

18 Verify that the displays essential for operator action provide direct or immediate trend or rate information. Trend information essential for operator action should be being continuously available on dedicated trend displays and selectively available on other displays that provide redundancy. Those essential display systems should have the capability of providing at least 30 minutes of data and have recording capability.

19 Verify that those measured variables that pertain to accomplishing or maintaining critical safety functions, those needed for manual control, those needed for determining fuel breach magnitude, and those that can be used in determining the magnitude of radioactive release are recorded for future use. Data recording may be continuously updated, stored in electronic memory, and displayed on demand with the capability for at least 30 minutes of pre-event and 12 hours of post-event logging.

Quality

20 Verify that the quality of the components and equipment in the radiation monitoring systems are commensurate with their safety importance.

Use of Digital Systems

21 Verify that the software in the radiation monitoring system was developed under a software management program commensurate with the risk associated with its failure or malfunction.

22 To provide assurance that the required computer system hardware and software are installed in the appropriate system configuration, verify that the licensee has a program to ensure that the correct version of the software/firmware is installed in the correct hardware components.

23 Verify that the tests for digital computer system equipment for the radiation monitoring systems are comprehensive and show that the system can perform its required functions should be provided.

24 Verify that the reliability of the digital computer system equipment for the radiation monitoring systems, if given, is reasonable and is based on a combination of analysis, field experience, testing, or software error recording and trending.

Cyber Security

25 Verify that the licensee has adequately addressed potential security vulnerabilities in each phase of the digital safety system lifecycle. The lifecycle phase-specific security requirements should be commensurate with the risk and magnitude of the harm resulting from unauthorized and inappropriate access, use, disclosure, disruption, or destruction of the digital safety system.

Review Procedures

The reviewer should confirm that the design bases for the radiation monitoring systems and equipment I&Cs are consistent with giving reliable indication of the presence of radiation or release of radioactive material in the various areas monitored and in the monitored effluent streams from the reactor. The reviewer should establish that the design includes sufficient monitoring systems and equipment to perform the functions discussed elsewhere in the SAR. The reviewer should compare the equipment and designs and functions with the design bases and acceptance criteria. The reviewer should obtain the assistance of experts in the I&C Branch to review computer systems.

Evaluation Findings

This section of the SAR should include sufficient information to support the following types of conclusions, which will be included in the staff's safety evaluation report (the second and third conclusions may be presented in Section 11.1.4):

1. The designs and operating principles of the instrumentation and control of the radiation detectors and monitors have been described, and have been shown to be applicable to the anticipated sources of radiation.

2. The staff found that the SAR discusses all likely radiation and radioactive sources anticipated at the (insert name of facility) and describes equipment, systems, and devices that will give reasonable assurance that all such sources will be identified and accurately evaluated.
3. The radiation monitoring systems described in the SAR give reasonable assurance that dose rates and effluents at the facility will be acceptably detected, and that the health and safety of the facility staff, the environment, and the public will be acceptably protected.

7.8 References

1. American National Standards Institute/American Nuclear Society, ANSI/ANS 10.4, “Guidelines for the Verification and Validation of Scientific and Engineering Computer Programs for the Nuclear Industry,” ANS, LaGrange Park, Illinois, 1987.

2. American National Standards Institute/American Nuclear Society, ANSI/ANS 15.15, "Criteria for the Reactor Safety Systems of Research Reactors," ANS, LaGrange Park, Illinois, 1978. (withdrawn)

3. American National Standards Institute/American Nuclear Society, ANSI/ANS 15.20, “Criteria for the Control and Safety Systems for Research Reactors” (draft), ANS, LaGrange Park, Illinois.

4. American Nuclear Society, *Transactions of the American Nuclear Society, Session on Digital Control of Nuclear Reactors*, Vol. 64, pp. 248-259, San Francisco, California, November 10-14, 1991.

5. Institute of Electrical and Electronics Engineers, IEEE Standard 7-4.3.2-2003, “IEEE Standard Criteria for Digital Computers Systems in Safety Systems of Nuclear Power Generating Stations,” Piscataway, New Jersey, 1993.

6. U.S. Nuclear Regulatory Commission, “Use of NUMARC/EPRI Report TR-102348, 'Guideline on Licensing Digital Upgrades, in Determining the Acceptability of Performing Analog-to-Digital Replacements Under 10 CFR 50.59',” Generic Letter 95-02, April 26, 1995.

7. U.S. Nuclear Regulatory Commission, “NRC Regulatory Issue Summary 2002-22: Use Of EPRI/NEI Joint Task Force Report, “Guideline on Licensing Digital Upgrades: EPRI TR-102348, Revision 1, NEI 01-01: A Revision of EPRI TR-102348 to Reflect Changes to the 10 CFR 50.59 Rule,” November 25, 2002.

8. U.S. Nuclear Regulatory Commission, NRC Information Notice 2010-10, “Implementation of a Digital Control System Under 10 CFR 50.59,” May 28, 2010.