7 INSTRUMENTATION AND CONTROL SYSTEMS

This document describes acceptable format and content of the safety analysis report (SAR) to be submitted to the U.S. Nuclear Regulatory Commission (NRC) by an applicant or licensee of a non-power reactor for a new license, license renewal, or license amendment. A companion document, NUREG-1537, Part 2 (Standard Review Plan), gives criteria to assist NRC staff reviewers in effecting comparable, complete, and consistent reviews of licensing applications for non-power reactors.

The guidance herein is based on Title 10 of the *Code of Federal Regulations* (10 CFR) Section 50.34, which describes the information to be supplied in a SAR.

In this chapter of the SAR the applicant describes and discusses the design and operating characteristics of the instrumentation and control (I&C) systems. Sufficient information should be included to explain the design criteria and bases, and to discuss the functional and safety analyses of the I&C subsystems. The I&C subsystems generally comprise the reactor control system (RCS), process instruments, the reactor protection (safety) system (RPS), instruments to initiate operation of engineered safety features (ESFs), and radiation safety monitoring systems. These systems and their outputs can be consolidated into a control console, along with the devices and circuits that control the operation of the reactor. The guidance in this chapter of the SAR is based on the principle that most non-power reactors can be designed and operated to pose acceptably small or insignificant risk to the public without isolating or separating the RPS from other subsystems. Additional design features, such as separation' of systems, may be necessary for high-power test reactors. Applicants who need additional guidance beyond that given in this chapter should contact their project manager.

The non-power RPS should monitor selected reactor operating parameters such as neutron flux; fuel temperature (monitored primarily in TRIGA-type reactors); primary coolant flow, temperature, and level; and radiation intensity. The RPS is designed to ensure reactor and personnel safety by limiting parameters to operate within analyzed operating ranges. The RPS can also give the ESF actuation system information for the operation of ESFs when the instruments indicate that abnormal or accident conditions could occur. The RCS may monitor many of the same parameters as the RPS and give information for automatic or manual control of the reactor operating conditions (e.g., reactor power, by inserting or withdrawing control rods). The reactor facility instruments present operating parameter and system status information to the operator for monitoring reactor operation and for deciding on manual control actions to be taken. Instrument systems are the means through which automatic or operator control actions are transmitted for execution by the RCS. Radiation instruments show radiation levels in selected areas in the reactor facility and could give data to the RPS, give information to help in the control of personnel radiation exposure, or monitor the release of radioactive material from the reactor and the reactor building.

In this chapter, the applicant should discuss the functional requirements, design criteria and bases, system descriptions, system performance analyses, and the bases of technical specification limiting safety system settings (LSSSs), limiting conditions of operation (LCOs), and surveillance requirements for the I&C systems for non-power reactors.

10 CFR 50.59(c)(1) permits licensees to make changes in the facility as described in the final safety analysis report (as updated), make changes in the procedures as described in the final safety analysis report (as updated), and conduct tests or experiments not described in the final safety analysis report (as updated) without obtaining a license amendment pursuant to 10 CFR 50.90 only if:

I. A change to the technical specifications incorporated in the license is not required, and

II. The change, test, or experiment does not meet any of the criteria in paragraph 10 CFR 50.59(c)(2).

A licensee should obtain a license amendment pursuant to 10 CFR 50.90 prior to implementing a proposed change, test, or experiment if the change, test, or experiment would result in an increase in the likelihood or consequence of an accident or introduce a previously unanalyzed accident. Regulatory Guide (RG) 1.187 provides guidance for the implementation of 10 CFR 50.59, changes, tests, and experiments, including that for non-power reactors (Regulatory Position C.5). NEI 01-01, which updates Electrical Power Research Institute (EPRI) Report TR-102348, is endorsed by Regulatory Issue Summary (RIS)-2002-22 and complements NEI 96-07 by explicitly addressing digital upgrade issues. (The original version of EPRI TR-102348 was endorsed by Generic Letter (GL) 95-02, with clarifications.) For I&C systems that are being upgraded (including systems based on digital technology), the applicant may consult NEI 96-07 and NEI 01-01. While most of the examples and specific discussion focus on power reactors, the guidance contained in Revision 1 of NEI 96-07 is also applicable to evaluations performed by licensees for non-power reactors. NEI 01-01 by proposes ways to address and resolve digital-specific issues in the design and evaluation process. A license amendment request (LAR) is required for any changes to the Technical Specifications (TSs). For example, if the safety analysis credits the trip and the upgrade is to a digital I&C system, a LAR would be required. Guidance on the need for a LAR and performance of a 10 CFR 50.59 review is provided in NEI 96-07 and NEI 01-01.

7.1 Summary Description

In this section of the SAR, the applicant should briefly describe the I&C systems of the reactor, including block, logic, and flow diagrams showing major components and subsystems, and connections among them. The applicant should summarize the technical aspects, safety, philosophy, and objectives of the I&C system design and should discuss such factors as redundancy, diversity, and isolation of functions. The information should include:

- Type of instruments-System instruments should be described by type [e.g., hardwired analog, computerized digital that uses stored programs (software) or combinations of these]. If a combination is used, the applicant should clearly note which portions or functions are analog and which are computerized digital, and how they relate to each other. The applicant could refer to existing systems reviewed and approved by NRC that are similar to the described system.

- Classification of systems-I&C systems and equipment should be classified into categories by function performed (e.g., the RCS, RPS, ESF actuation system, control console and display instrument systems, and radiation protection instruments).

The general description of each category of I&C subsystem should include the following, as applicable:

- For the RCS, a brief discussion of each major subsystem such as manual control system, automatic control system, control rod drive systems, bypass and interlock systems, and any integrated experiment I&C systems.

- For the RPS, the types of parameters monitored, both nuclear and nonnuclear, the number of channels designed to monitor each parameter, the actuating logic that determines the need for actions to change reactor conditions and that takes these actions, and number and type of reactivity control devices.

- For the ESF actuation system, a discussion of the subsystems that detect the need for operation and that initiate operation including identification of the parameters monitored or the source of input information and the number of channels designed to monitor, process, and act on the information.

- For the control console and display instruments, a discussion of the parameter display systems and equipment by which the operator can observe and control the operation of the reactor and important subsystems.

- For radiation protection instruments, a brief discussion of area and effluent radiation detection systems that monitor, alarm, or provide input to other subsystems of potentially hazardous radiation levels. The applicant should address radiation system that monitor effluent streams from the reactor facility, state the type of effluent (such as airborne or liquid), and list alarms or signals to other subsystems.

- A summary of the human-machine interface principles used in the location of instrumentation and controls.

7.2 Design of Instrumentation and Control Systems

10 CFR 50.34(a) describes the information to be supplied in a PSAR while 10 CFR 50.34(b) describes the information to be supplied in an FSAR. More specifically, 10 CFR 50.34(a)(3)(i) requires applicants to provide the principal design criteria for the facility and 10 CFR 50.34(a)(3)(ii) requires applicants to describe the design bases and the relation of the design bases to the principal design criteria.

The SAR should address the following:

- design criteria

- design bases

- system description

- system performance analysis

- conclusion

Guidance for the review of a digital upgrade under 10 CFR 50.59 is provided in Section 7.2.6.

7.2.1 Design Criteria

In this section of the SAR, the applicant should ~~discuss~~ describe the criteria for developing the design criteria for the I&C systems. (The design criteria for the facility are described in Section 3.1.)

10 CFR 50.34(a)(3)(i) requires applicants to provide the principal design criteria for the facility.

The principal design criteria establish the necessary design, fabrication, construction, testing, and performance requirements for structures, systems, and components important to safety; that is, structures, systems, and components that provide reasonable assurance that the facility can be operated without undue risk to the health and safety of the public.

Types of design criteria that should be considered include, but are not limited to:

1. Consideration of the need to design against single failures (e.g., I&C systems should be designed so that a single failure will not prevent the safe shutdown of the reactor),

2. Consideration of redundancy and diversity requirements,

3. Consideration of the type, size, and orientation of possible breaks in components of the reactor coolant boundary in determining design requirements to suitably protect against postulated loss-of-coolant accidents, and

4. Consideration of the possibility of systematic, nonrandom, concurrent failures of redundant elements in the design of protection systems and reactivity control systems.

The basis for evaluating the reliability and performance of the I&C systems should be included. 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. Where generally recognized codes and standards are used, they should be named and evaluated for applicability, adequacy, and sufficiency.

The basis for evaluating the reliability and performance of the I&C systems should be included. 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. Where generally recognized codes and standards are used, they should be named and evaluated for applicability, adequacy, and sufficiency. They should be supplemented or modified as needed in keeping with the safety importance of the function to be performed.' Evaluations and modifications of the standards should be described in the SAR. A set of generally applicable criteria for use as a guide is given below. Criteria that are used should be clearly stated and should be shown to provide the appropriate level of reliability, safety, and performance capability. The applicability of these criteria should be determined from the operating analyses in Chapter 4, 'Reactor Description," and accident analyses in Chapter 13, "Accident Analyses," of the SAR.

- Systems and components (including I&C systems) determined by the analyses in the SAR to be important to the safe operation or shutdown of the reactor should be designed to be in accordance with local building and siting codes, and should be able to withstand the effects of natural phenomena without loss of capability to perform their safety function (see Chapter 3, 'Design of Structures, Systems, and Components," for additional information).

- I&C systems and components determined in the SAR analyses to be important to the safe operation or shutdown of the reactor should be designed, located, and protected so that the effects of fires or explosions would not prevent them from performing their safety functions.

- I&C systems and components determined in the SAR to be important to the safe operation or shutdown of the reactor should be designed to function reliably under anticipated environmental conditions (e.g., temperature, pressure, humidity, and corrosive atmospheres) for the full range of reactor operation, during maintenance, while testing, and under postulated accident conditions, if the systems and components are assumed to function in the accident analysis.

- The RPS should be designed to automatically initiate the operation of systems or give clear warning to the operator to ensure that specified reactor design limits are not exceeded as a result of measured parameters indicating the onset of potential abnormal conditions. The ESF actuation system should be designed to automatically initiate operation to mitigate the consequences of abnormal conditions or accidents.

- I&C systems should be designed to have functional reliability, including redundancy and diversity, commensurate with the safety functions to be performed and the consequences of failure of the system to perform the safety function. For example, an I&C system for a non-power reactor should be designed to perform its protective function after experiencing a single random active failure within the system.

- I&C systems should be designed to fail into a safe state on loss of electrical power or exposure to extreme adverse environments.

- I&C systems should be designed so that a single failure will not prevent the safe shutdown of the reactor.

7.2.2 Design-Basis Requirements

I&C system design requirements for non-power reactors are generally derived from the results of analyses of normal operating conditions and of accidents and transients that could occur.

10 CFR 50.34(a)(3)(ii) requires applicants to describe the design bases and the relation of the design bases to the principal design criteria.

Design bases means that information which identifies the specific functions to be performed by a structure, system, or component of a facility, and the specific values or ranges of values chosen for controlling parameters as reference bounds for design. These values may be (1) restraints derived from generally accepted "state of the art" practices for achieving functional goals, or (2) requirements derived from analysis (based on calculation and/or experiments) of the effects of a postulated accident for which a structure, system, or component must meet its functional goals.

The design bases should identify modes of operation, environmental parameters, safety functions, permissive conditions, variables to be monitored and their ranges, conditions for manual control, and any other special design bases that may be imposed on the system design (e.g., interlocks). For example, the modes of operation at a facility may require a period meter; this should be identified in the design basis because some pulse reactors may not need a period meter. For the control system, the design bases should demonstrate that the RCS is not required for safety.

The design basis should address the following characteristics:

- Completeness - The design basis should address all system functions necessary to fulfill the system's safety intent. Information provided for each design basis item should be sufficient to enable the detailed design of the I&C system to be carried out. All functional requirements for the I&C system and the operational environment for the I&C system should be described. As a minimum, each of the design basis aspects identified in ANSI/ANS 15.15-1978 should be addressed.

- Consistency - The information provided in the design basis should be analyzed to demonstrate its consistency with the facility’s safety analysis, including the maximum hypothetical accident analysis of Chapter 13 of the SAR; the mechanical and electrical system designs; and other system designs.

The design bases for software should address the following characteristics:

- Correctness - The information provided for the design basis items should be technically accurate.

- Traceability - It should be possible to trace the information in each design basis item to the safety analyses, facility’s system design documents, regulatory requirements, applicant/licensee commitments, or other documents.

- Unambiguity - The information provided for the design basis items, taken alone and in combination, should have one and only one interpretation.

- Verifiability - The information provided for the design basis items should be stated or provided in such a way as to facilitate the establishment of verification criteria and the performance of analyses and reviews of the various safety systems.

This section provides guidance on the factors to consider in developing the analyses and the design bases. Design bases for the I&C system, subsystems, and components should include the following, as applicable:

- The function or purpose of systems or instruments considering which reactor parameters are monitored or controlled.

- The range of values that monitored variables may exhibit for normal operation, shutdown conditions, and for postulated accidents.

- Safety or control functions and any unique or facility-specific functions performed by the I&C system or subsystems.

- Specification of alarm, trip, and actuation setpoints derived from accident or other operational analyses of the instrumented system or function.

- Any special requirements such as redundancy, diversity, quality assurance, and environmental requirements 'derived from the results of analyses of the full range of operating conditions and postulated accidents.

- The specification of precision and accuracy requirements for the instruments, control subsystems, or components.

- The specification of number and type of channels required to monitor variables.

- The system operational and support requirements such as those for electrical, mechanical, structural, cooling, heating, and signal input.

- The requirements that controls and instruments be grouped and located so that operators can easily reach and manipulate the controls while readily observing on meters and displays the results of their actions (operator interface requirements).

- Each clause in IEEE 7-4.3.2-2003 and RG 1.152, R3 were reviewed for applicability on a section-by-section basis. If review guidance (Part 1)/acceptance criteria (Part 2) matching the intent of that clause was not addressed it was “expanded” into the list of criteria.
- Removed the references to GL 95-02 in Sections 7.3-7.7; updated the reference and moved discussion of guidance for a digital upgrade to the beginning of Section 7.2.

7.2.3 System Description

The system description in the SAR should include equipment and major components as well as block, logic, and schematic diagrams.

Title 10, Section 50.34(a) of the Code of Federal Regulations describes the information to be supplied in a PSAR while 50.34(b) describes the information to be supplied in an FSAR. The range of the sensors should cover the range of the accidents.

All applications should provide sufficient detail to allow an evaluation on the basis of their technical content and completeness. The system description of the RCS should include equipment and major components as well as block, logic, and schematic diagrams, including hardware and software descriptions and software flow diagrams for digital computer-based systems. The descriptions should also address how the system operational and support requirements will be met and how the operator interface requirements will be met. The applicant should include a description of the design criteria for the RCS as outlined in Section 7.2.3 (Part 1), including any additional system descriptive material specific to subsystem design and implementation not covered in Section 7.2.

The applicant should also submit hardware and software descriptions and software flow diagrams for digital computer systems. The applicant should describe how the system operational and support requirements will be met and how the operator interface requirements will be met. The description should also address the methodology and acceptance criteria used to establish and calibrate the trip or actuation setpoints, or interlock functions.

7.2.4 System Performance Analysis

The applicant should conduct a performance analysis of the proposed I&C system to ensure the design criteria and design bases are met and license requirements for the performance of the system are specified. The system performance analysis should encompass the following:

- The SAR should describe the operation of the I&C system and present the analysis of how the system design meets the design criteria and design bases. The discussion should include accuracy, reliability, adequacy and timeliness of I&C system action, trip setpoint drift, quality of components and, if required by the analyses, redundancy, independence, and how a single failure affects both its ability to perform its safety function and the effect on operation or safe shutdown of the reactor.

- Technical specification LSSSs, LCOs, and surveillance requirements for the I&C system should be established. These parameters and requirements should include system operability tests, trip or actuation setpoint checks, trip or actuation-setpoint calibrations, and any system response-time tests that are required. Surveillance intervals should be specified and the bases for the intervals, including operating experience, engineering judgment, or vendor recommendation should be described.

7.2.5 Conclusion

The applicant should summarize in this section of the SAR why the system design is sufficient and suitable for performing the functions stated in the design bases.

7.2.6 Digital Upgrades

When modifying an I&C system or upgrading from an analog to a digital I&C system, there are two possible conclusions to a 10 CFR 50.59 evaluation:

1. The proposed activity may be implemented without prior NRC approval.

2. The proposed activity requires prior NRC approval and the licensee must submit a license amendment request and needs to receive approval prior to implementation.

In 1995, the NRC issued GL 95-02, which endorses EPRI Report TR-102348, "Guideline on Licensing Digital Upgrades" for providing acceptable guidance for determining when an analog-to-digital replacement can be performed without prior NRC staff approval under the requirements of 10 CFR 50.59. The EPRI report applies to all digital equipment that uses software and, in particular, to microprocessor-based systems.

In 2002, the NRC issued RIS 2002-22, which endorses EPRI TR-102348, Rev. 1/NEI 01-01 (EPRI 1002833), an update to the original EPRI TR-102348 endorsed in GL 95-02. EPRI TR-102348 was updated to reflect the revised 10 CFR 50.59 rule and the industry guidance for implementing this rule (i.e., NEI 96-07, Revision 1, which was endorsed by RG 1.187). The NRC staff has reviewed this report and has concludes that it provides suitable guidance both for designing a digital replacement and for determining whether it can be implemented under 10 CFR 50.59 without prior staff approval.

It is not the intent of the EPRI/NEI report or of the NRC staff to predispose the outcome of the 10 CFR 50.59 process, but rather to provide a process that will assist licensees in reaching a proper conclusion regarding the existence of an unreviewed safety question when undertaking a digital system replacement. The licensee determines (per 10 CFR 50.59) if the change requires a review by the NRC (per10 CFR 50.90); however, the applicant should consider current 50.59 experiences (for example, IN 2010-10). Currently most I&C changes should be reviewed and licensee should consult with the NRC Project Manager (PM) for the latest applicable guidance.

Although not all digital equipment replacement usage will automatically result in an unreviewed safety question, it is likely that digital modifications to safety-significant systems such as the RPS or ESF actuation system will require staff review.

Some potentially adverse effects that should be evaluated include:

- Replacing analog with digital equipment
  - software common-cause failures cannot be assumed to be incredible failures
  - a digital system can fail “fixed” without giving any indication that it has failure
  - a watchdog timer may add diversity and redundancy but does add a new failure mode
- Combining previously separate functions into one digital device such that failures create new malfunctions (i.e., multiple functions are disabled if the digital device fails)
- Changing performance from SAR-described requirements (e.g., for response time, accuracy, etc.)
- Changing functionality in a way that increases complexity, potentially creating new malfunctions
- Introducing different behavior or potential failure modes that could affect the design function
- Changes that fundamentally alter (replace) the existing means of performing or controlling design functions
  - replacement of automatic action by manual action (or vice versa)
  - changes to the man-machine interface
  - changing a valve from "locked closed" to "administratively closed"
  - similar changes

- HSI changes that could lead to potential adverse effects
  - Changes to parameters monitored, decisions made, and actions taken in the control of plant equipment and systems during transients
  - Changes that could affect the overall response time of the human/machine system (e.g., changes that increase operator burden)
  - Fundamental changes in data presentation (such as replacing an edgewise analog meter with a numeric display or a multipurpose CRT where access to the data requires operator interactions to display)
  - Changes that create new potential failure modes in the interaction of operators with the system (e.g., new interrelationships or interdependencies of operator actions and plant response or new ways the operator assimilates plant status information)

If a simple component (no digital communication) has been approved for use under an Appendix B program for a nuclear power plant, it is good enough to be used at an NPR and screened out under a 50.59 review. However, the 8 questions in 10 CFR 50.59 must still be answered to address if the replacement introduces a new failure mode. (The simple components use must be consistent with the original use.)

7.3 Reactor Control System

The RCS performs several functions, such as maintaining the reactor in a shutdown state, reactor startup, changing power levels, maintaining operation at a set power level, and shutting down the reactor. In non-power reactor designs that allow pulsing (such as the TRIGA design); the RCS can rapidly insert reactivity into the reactor core to produce a predetermined high-power pulse of short duration, or to achieve a rapid increase in reactor power in a "square wave." The RCS may be discussed using such subsystems as nuclear instruments, process instruments, control elements, and interlocks. In describing each subsystem in the SAR, the applicant should include design considerations and technical specification requirements.

In the nuclear instrument system, nuclear instruments monitor the neutron flux from the subcritical source multiplication range, through the critical range, and' through the intermediate flux range to full power. Neutron flux instruments also should determine the startup rate and, in some designs, reactor period information.

Linear and log neutron flux channels should be used to monitor the core neutron flux while control rods are withdrawn or inserted to increase or decrease reactor -power. At least one linear neutron flux channel should be calibrated to reactor thermal power.

The process instruments are 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. In some designs, this information may also be sent to the RPS.

The typical non-power reactor has an automatic control (servo) system that controls the reactor power about a point set by the operator. Most servo control systems compare the output of a linear neutron flux channel against an adjustable voltage representing the desired power level; and automatically change the position of a regulating rod in the core to change the neutron flux density to reduce the difference between the two voltages until the actual reactor power level is very nearly equal to the desired power level. This process can be performed by analog control equipment or by software in a digital computer system.

Reactors with pulsing capabilities have a transient rod that, on command, is rapidly ejected out of the core to a pre-programmed distance. This action rapidly inserts a known amount of excess reactivity into the core that pulses the core power to very high levels for very short intervals. The system can also be used to form a square wave power increase to a predetermined steady-state power level.

The RCS for non-power reactors should have a set of equipment protection interlocks and inhibits that prohibit or restrict operation of the reactor unless certain conditions are met. For example, there should be an interlock that prohibits control rod motion unless the neutron flux in the core produces a neutron count rate sufficient to help ensure that nuclear instruments are responding to neutrons. There may be additional equipment protection interlocks to ensure, for example, that there is sufficient coolant flow, shielding is intact, ventilation air is flowing, coolant level is sufficient, and required neutron instruments and recorders are functional. There may also be personnel protection interlocks to prevent reactor operation if certain radiation fields are excessive. Control rods may be run back to automatically reduce the reactor power when certain specified reactor conditions approach a predetermined limit, but total reactor shutdown (scram) is not warranted.

Experimental facilities may be interlocked with the RCS to prevent reactor operation if the experimental facility is not in the correct configuration. If experiments conducted in non-power reactors could interact with the core to change reactivity or otherwise modify the reactor operating conditions, data to the RCS or RPS from the experiment instruments may be needed to detect reactivity changes. All experiments should be carefully considered for interaction with the I&C system when the safety analysis for the experiment is performed. The analysis should consider any interaction with the RCS or RPS. Where such interactions are warranted, they should meet the standards used for the design of the systems to which the experimental facilities will be connected.

10 CFR 50.34(a) describes the information to be supplied in a PSAR while 10 CFR 50.34(b) describes the information to be supplied in an FSAR. More specifically, 10 CFR 50.34(a)(3)(i) requires applicants to provide the principal design criteria for the facility and 10 CFR 50.34(a)(3)(ii) requires applicants to describe the design bases and the relation of the design bases to the principal design criteria.

The applicant should include the following for each RCS subsystems:

- A description of the design criteria for the RCS as outlined in **Section 7.2.1**, including any criteria specific to the reactor design not outlined in the section.

- A description of the design bases information specified in **Section 7.2.2** and any additional design bases of facility-specific subsystems.

10 CFR 50.34(a)(3)(ii) requires applicants to describe the design bases and the relation of the design bases to the principal design criteria.

Design bases means that information which identifies the specific functions to be performed by a structure, system, or component of a facility, and the specific values or ranges of values chosen for controlling parameters as reference bounds for design. These values may be (1) restraints derived from generally accepted "state of the art" practices for achieving functional goals, or (2) requirements derived from analysis (based on calculation and/or experiments) of the effects of a postulated accident for which a structure, system, or component should meet its functional goals.

The design bases should identify modes of operation, environmental parameters, safety functions, permissive conditions, variables to be monitored and their ranges, conditions for manual control, and any other special design bases that may be imposed on the system design (e.g., interlocks). For example, the modes of operation at a facility may require a period meter; this should be identified in the design basis because some pulse reactors may not need a period meter. For the control system, the design bases should demonstrate that the RCS is not required for safety.

- A description of the system as specified in **Section 7.2.3**, including any additional system descriptive material specific to subsystem design and implementation not covered in Section 7.2.

- An analysis of the operation and performance of the system as specified in **Section 7.2.4** including analyses and results of any features or aspects specific to the facility design and implementation not specified in Section 7.2. The applicant should include the bases of any technical specifications and surveillance tests with intervals specific to the design and operation of the systems.

In its analysis of the operation and performance of the RCS, the applicant should address the specific design features of the RCS, such as the following:

Design Basis

The sensors in the RCS give~~s~~ a continuous indication of the neutron flux density from subcritical multiplication source level to the expected power ranges evaluated in other parts of the SAR. If multiple detector channels are used, this continuous indication should overlap a minimum of one decade during detector changeover.

Provide a description showing that the RCS would be capable of maintaining system variables (including the neutron flux density) within prescribed operating ranges over its anticipated range for normal operation (from subcritical multiplication source level through the full licensed power range), for postulated accidents, and for accident conditions. Include those variables used to assure adequate safety, including those variables and systems that can affect the fission process, the integrity of the reactor core, the reactor coolant pressure boundary, and the containment and its associated systems. Show that sensors adequately cover the range of operations and accident conditions and should be based on the accident conditions evaluated in Chapter 13.

The RCS design analysis includes verification that instrumentation and systems, along with the data processing systems and alarms, will reasonably assure operation within specified design limits. The analysis of the design should provide assurance that I&C systems can adequately monitor changes in core reactivity and maintain variables that affect core reactivity within designed operating ranges, thus minimizing the possibility of an adverse transient affecting the integrity of the primary fission product barrier (e.g., fuel cladding).

With respect to provision of I&C to monitor variables and systems that can affect the fission process, provide the following:

- A description of the analysis that demonstrates that suitable instrumentation and systems are provided to monitor the core power, control rod positions and patterns, and other process variables such as temperature and pressure, as applicable.

- A description of the analysis that demonstrates that suitable alarms and/or control room indications for these monitored variables are provided.

In addition, provide a description of the specific design features of the RCS should address the following:

- Detector channels directly monitor the neutron flux density for presentation of reactor power level and power rate-of-change.

- The RCS has at least two channels of reactor power indication through the licensed power range.

- The startup and operating power detector channels can discriminate against strong gamma radiation, such as that present after long periods of operation at full power, to ensure that indicated changes in neutron flux density are reliable.

- The reactor power indication of at least one channel should remain reliable for some predetermined range above the licensed power level. For reactors with power level as a safety limit, the instrumentation should be able to indicate if the safety limit was exceeded. For other reactor types, at least one channel should be able to indicate if the power level, which is the basis for limiting licensed power level, was exceeded.

- All control rod positions should be indicated at the control console throughout their travel and should indicate when they are at an "in" or "out" limit.

Provide a summary of the analysis used to verify the adequacy of control systems with respect to maintaining variables within operational limits during facility operation and to verify that the impact of control system failures is appropriately included in the maximum hypothetical accident analyses. The applicant should summarize in this section of the SAR why the system design is sufficient and suitable for performing the functions stated in the design bases.

Provide a description showing that RCS is designed for reliable operation in the normal range of environmental conditions anticipated within the facility. If environmental controls such as heat tracing of instrument lines or cabinet cooling fans are necessary to protect equipment from environmental conditions, these should also be described.

Maintaining system performance provides the basis for the technical specifications of non-power reactors (Ch. 14), consistent with the safety analysis with respect to reliability, availability, and capability of the RCS.

Provide a description showing that the capability of the RCS is addressed by limiting or enveloping conditions of design and operation, such as:

- The control rod drive speed in "manual" and "automatic" modes of operation should be limited to that analyzed and allowed for controlling the rate of change of reactivity.
- The RCS and the reactor reactivity control system should meet the requirements of minimum shutdown margin considering the stuck rod criteria.

Factors in experiments which could adversely affect control system features include:

a. Neutron flux perturbations affecting calibrations of safety channels and/or rod worths.

b. Mechanical forces adversely affecting shielding or confinement arising from causes as in mechanical forces on fuel cladding arising from the manipulation of experimental components, from tools used for such manipulation, from thermal stress, vibration, or shock waves, or from missiles arising from functioning or malfunctioning experiments.

c. Radiation fields or radioactive releases from experiments which can mask the performance of an operational monitoring system intended for the detection of fission product releases at early stages.

d. Physical interference by experiment components with reactor system components such as control or safety rods or physical displacement of reactor system shielding.

Provide a description of the factors in experiments that can adversely affect control system features and any associated technical specifications arising from experimental systems.

Provide a description of plans for installation of software on installed systems in operating facility's, recognizing the need to declare all affected functions inoperable according to the facility's technical specifications before proceeding with installation, and to conduct appropriate return-to-service testing before declaring the modified function operable.

The RCS has a reactor period channel that covers subcritical neutron source multiplication from the approach to critical, through critical, and into the power range. Depending on the analysis in the SAR, some reactors may not have this channel.

If the design basis requires the use of period meters, provide a description showing that the reactivity control systems are designed with appropriate limits on the potential amount and rate of reactivity increase to assure that the effects of postulated reactivity accidents cannot impair significantly the capability to cool the core. These postulated reactivity accidents should include consideration of reactivity addition accidents (e.g., ramp, pulse, experiments, etc.), as applicable.

Provide a description showing that any single control system component or channel, or failure or removal from service of any single component or channel in the RPS, which is common to the RCS and RPS systems, should leave intact a system satisfying all reliability, redundancy, and independence requirements of the RPS.

In a reactor designed for pulsing, provide an analysis that shows that the movement of the transient rod is limited in accordance with reactivity amounts and rates derived from the SAR analysis.

In a reactor designed for pulsing, provide a description of the system indication for the position of the transient rod, when this rod is fully inserted, and when it is set in position to initiate a pulse, and describe the interlocks to ensure the position of the rod.

The features for manual and automatic control facilitate the capability to maintain facility variables within prescribed operating limits. Provide a description of how the control systems permit actions to be taken to operate the facility safely during normal operation, including postulated accidents.

The control console and display system should indicate the mode of operation. For example, the RCS should indicate the operating mode, status and change of status of the reactor control mode at all times for facilities with any automatic control modes.

Provide a description of the displays available to the operator indicating the mode of operation, status, and change of status for automatic and manual control.

Design Criteria

Independence

If the RCS and RPS are designed to be independent systems, the issues of independence are physical, electrical, communications, and functional independence. The use of digital I&C add unique independence issues related to communication independence and functional independence.

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 common 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 combining the two systems, they need not be separate, independent, or isolated from each other. The RPS design should be 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. Isolation devices between the safety system and a non-safety system are classified as part of the safety system.

Provide a description of the physical, electrical, and communications independence of the RCS from the RPS. The description should be sufficient to show that the safety system design precludes the use of components that are common to redundant portions of the safety system, such as common switches for actuation, reset, mode, or test; common sensing lines; or any other features which could compromise the independence of redundant portions of the safety system. Physical independence is attained by physical separation and physical barriers.

Fail Safe

The system and equipment are designed to assume a safe state on loss of electrical power.

Provide a description of the safe state for a loss of electrical power and those components that should change state for these conditions.

Effects of control system operation/failures

The conclusions of the analysis of postulated accidents and accidents as presented in Chapter 13 of the SAR are used to verify that facility safety is not dependent upon the response of the control systems. In addition, failure of the control systems themselves or as a consequence of supporting system failures, such as loss of power sources, should not result in facility conditions more severe than those described in the analysis of maximum hypothetical accident and postulated accidents. Show that the accidents analyzed in Chapter 13 of the SAR do not depend on the operability of the RCS to assure safety.

If the RCS and RPS are separate systems, the safety functions should be placed with the RPS. This requirement does not apply to a combined RCS-RPS.

Provide a summary of potential accidents analyzed in Chapter 13 of the SAR, identifying those I&C systems necessary to preclude and/or mitigate those accidents.

The RCS protects against a failure or operation in a mode that could prevent the RPS from performing its intended safety function. The design of the control system should consider the following:

- effects of control system operation upon accidents,
- effects of control system failures, and
- effects of control system failures caused by accidents.

Provide a description showing that the failures of any control system component or any auxiliary supporting system for control systems are bounded by the analysis of postulated accidents in Chapter 13 of the SAR. While failure analyses typically address random hardware failures, this evaluation should also address failure modes that could be associated with software failures.

The SAR should contain a review of the consequential effects of postulated accidents and accidents are bounded by the accident analysis in Chapter 13 of the SAR. Finally, the review should summarize the safety analysis regarding consideration of the effects of both control system action and inaction in assessing the transient response of the facility for accidents and postulated accidents.

Operational Bypass

Bypasses of interlocks should be under the direct control of the reactor operator and should be indicated in the control room. The need for, and potential consequences of bypassing interlocks should be carefully evaluated in the SAR.

Provide a description of the interlocks on such systems as the following, including provisions for testing and bypassing, if shown to be acceptable: transient rod drives; power level or reactor period recorders; startup neutron counter, gang operation of control elements; coolant flow or temperature conditions; beam ports, thermal column access, irradiation chambers, pneumatic or hydraulic irradiators, high radiation areas; confinement or containment systems; experiment arrangements and beam lines; or special annunciator or information systems. Interaction with the RPS, if applicable, should be described.

Direct interacting or interlocking with reactor controls may be justified if analyses of an experiment or experimental facility could show hazard to itself or the reactor. Any such automatic limiting devices should demonstrate that function of the RPS will not be compromised, or safe reactor shutdown will not be prevented (see Chapter 10, "Experimental Facilities and Utilization”).

Provide a description of those conditions in which experiment controls can interact with reactor controls.

Surveillance

To maintain reliable and accurate performance, I&C systems undergo testing and calibration. Calibration, especially in analog systems, is used to address instrument drift, inaccuracies, and errors. The performance of analog systems can typically be predicted by the use of engineering models. Digital I&C systems are fundamentally different from analog I&C systems in that minor errors in design and implementation can cause them to exhibit unexpected behavior. Inspection and testing are used to verify correct implementation and to validate desired functionality of the final product, in both analog and digital systems.

One benefit of digital I&C systems is the use of self-testing, which is a test or series of tests performed by a device upon itself. Self-tests include on-line continuous self-diagnostics, equipment-initiated self-diagnostics, and operator-initiated self-diagnostics. Self-testing can be used to ensure reliable and accurate performance.

Surveillance tests are conducted specifically to verify compliance with technical specification surveillance requirements.

Provide a summary of the calibration, inspection, and testing (including self-tests and surveillance tests) to validate the desired functionality of the system.

Provide a description of 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

10 CFR 50.55a(a)(1) requires that structures, systems, and components be designed, fabricated, erected, constructed, tested, and inspected to quality standards commensurate with the importance of the safety function to be performed. The design of the control system should be of sufficient quality to limit the potential for inadvertent actuation and challenges to safety systems. While the design of a control system that minimizes inadvertent actuations and challenges to a safety system is good practice, there is no specific requirement for such design practice in reactor applications for which no transients occur. That is, inadvertent actuation may not be a concern for research reactors below 2 MW and TRIGAs. Provide a description of the quality program for the RCS.

Managerial and administrative controls are used to assure safe operation. 10 CFR 50.34(a)(7) requires that applicants for construction permits describe a quality assurance program for the design and construction of the structures, systems, and components of the facility. 10 CFR 50.34(b)(6)(ii) requires a description in the SAR of managerial and administrative controls to be used to ensure safe operation. ANSI/ANS 15.8-1995, endorsed by RG 2.5, provides an acceptable method in developing a quality assurance program for the design, construction, testing, modification, and maintenance of research and test reactors for complying with the program requirements of 10 CFR 50.34.

Provide a description of the overall quality assurance program requirements. The program should identify the items and activities to which it applies and the extent of program application for each item and activity. The program should provide for the appropriate and necessary indoctrination and training of personnel who perform activities that affect quality, to ensure that suitable proficiency is achieved and maintained.

Use of Digital Systems

Digital I&C systems require additional design and qualification approaches than are typically employed for analog systems. The performance of analog systems can typically be predicted by the use of engineering models. These models can also be used to predict the regions over which an analog system exhibits continuous performance. The ability to analyze design using models based on physics principles and to use these models to establish a reasonable expectation of continuous performance over substantial ranges of input conditions are important factors in the qualification of analog systems design. These factors enable extensive use of type testing, acceptance testing, and inspection of design outputs in qualifying the design of analog systems and components. If the design process assures continuous behavior over a fixed range of inputs, and testing at a finite sample of input conditions in each of the continuous ranges demonstrates acceptable performance, performance at intermediate input values between the sampled test points can be inferred to be acceptable with a high degree of confidence.

Digital I&C systems are fundamentally different from analog I&C systems in that minor errors in design and implementation can cause them to exhibit unexpected behavior. Consequently, the performance of digital systems over the entire range of input conditions cannot generally be inferred from testing at a sample of input conditions. Inspections, type testing, and acceptance testing of digital systems and components do not alone accomplish design qualification at high confidence levels. To address this issue, the staff's approach to the review of design qualification for digital systems focuses to a large extent on verifying that the applicant/licensee employed a high-quality development process that incorporated disciplined specification and implementation of design requirements. Inspection and testing are used to verify correct implementation and to validate desired functionality of the final product, but confidence that isolated, discontinuous point failures will not occur derives from the discipline of the development process.

Failures in the control system failures cannot have an adverse effect on safety system functions and will not pose frequent challenges to the safety systems. The design of the control system design should be consistent with the commitments for control system/safety system independence. Isolation of safety systems from control system failures should be addressed. The topics to be covered for the control system include identifying the functional requirements, the development process, the process implementation, and the design outputs.

The control system software should be developed using a structured process similar to that applied to safety system software. The software development process should address potential security vulnerabilities in each phase of the software lifecycle.

Provide a description of the software development activities. If the software or system development was delegated to others, the authority, duties, verifying, and any activities that can affect the safety-related functions should be discussed.

Access Control

Access control, which includes physical and electronic control, applies to both analog and digital systems. Controls for physical access include provisions such as alarms and locks on panel doors, or administrative control of access to rooms. Access control includes both preventing unauthorized access but also allowing authorized access.

The objective of access control include protection of information and property from theft, corruption, or natural disaster, while allowing the information and property to remain accessible and productive to its intended users.

Access control and cyber security should be addressed throughout the software life cycle. The framework for the waterfall life cycle model consists of the following phases:

1. concepts,
2. requirements,
3. design,
4. implementation,
5. test,
6. installation, checkout, and acceptance testing,
7. operation,
8. maintenance, and
9. retirement.

Review of digital computer-based systems should consider controls that govern electronic access to system software and data. Provide a description of the controls used to address local and remote access. Examples of local access include access via maintenance equipment (e.g., workstations) and portable/removable storage devices. Examples of remote access include access via network connections. Special attention should be given to prevent inadvertent re-entry of outdated, superseded, or archived software versions into currently operating control equipment. Software and data updates should be verifiable by a version revision number and means for point-by-point validation of software.

Network connections may be allowed to experimental controls provided proper communications barriers provide adequate confidence that the nonsafety portions cannot interfere with performance of the safety portion of the software or firmware. Provide a description of any network connections and those controls used to prevent attacks and protect information.

For a combined RPS/RCS, the RCS should meet the requirements for the RPS.

Provide a description of those provisions to prevent unauthorized access to hardware and software, throughout the life cycle, for the RPS.

Cyber Security

Cyber security refers to preventative methods to protect information from attacks. It requires an understanding of potential information threats, such as viruses and other malicious code. The specific security requirements and subsequent review(s) are 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. Cyber security strategies include identity management, risk management and incident management.

The digital safety system development process should identify and mitigate potential weakness or vulnerabilities in each phase of the digital safety system life cycle that may degrade the Secure Development and Operational Environment (SDOE) or degrade the reliability of the system.

Provide a description of the cyber security program for the RCS.

- A description of the conclusions about capability and suitability of the RCS requested in **Section 7.2.5**. That is, the applicant should summarize in this section of the SAR why the system design is sufficient and suitable for performing the functions stated in the design bases.

7.4 Reactor Protection System

The RPS is designed to detect the need to place the reactor in a subcritical, safe shutdown condition (scram) when any of the monitored parameters exceeds the limit as determined in the SAR Upon detecting the need, the RPS should promptly and automatically place the reactor in a subcritical, safe-shutdown condition (scram) and maintain it there. This prevents or mitigates unintended operation in regions where risks of the following types could occur: fuel damage from overpower or loss of cooling events, uncontrolled release of radioactive materials to the unrestricted environment, or overexposure of personnel to radiation. Parameters monitored for this purpose could include core neutron flux, fuel temperature, core coolant flow and temperature, coolant level, area radiation levels, and air concentration, or release, of radioactive materials.

Non-power reactors can be designed and operated so that postulated accidents pose risks to the facility or the public that are not significant or that are within applicable regulatory limits. If justified by the accident analyses of Chapter 13, the RPS need not be separate and independent of the RCS. The applicant for such reactors may perform an analysis to determine whether certain RPS-monitored parameters or interlocks should be required to be redundant, diverse, or single-failure-proof. Two examples of these parameters are the reactor pool level or area radiation exposure rates. Therefore, the RPS and its subsystems should be designed in accordance with the guidance in Section 7.2, and the SAR should include the following information:

- A description of the design criteria for the RPS as outlined in **Section 7.2.1**, including any criteria specific to the reactor design not outlined in the section.

- A description of the safety and system design bases information as specified in **Section 7.2.2**. Any supplemental facility-specific design bases not specified in the general system requirements should be included.

- System descriptions consistent with that specified in **Section 7.2.3**, along with any subsystem description that is facility specific and that may not be identified in the general system requirements.

- Analyses of the operation and performance of the RPS similar to that specified in **Section 7.2.4**. This should include analysis of any features, aspects, or technical specifications including surveillance tests that may be reactor specific and not identified in the general system requirements. These analyses should be based on postulated credible accidents, transients, and other events that could require RPS intervention, and should include all of the applicable features noted in Section 7.3 for the RCS. The analyses should include quantitative performance of all scrams, runbacks, interlocks, and ESF initiators.

In its analysis of the operation and performance of the RPS, the applicant should address the following:

Design Basis

A log power level channel with a reactor period or rate-of-flux change output with a rate or period channel set to scram in accordance with the analysis (certain reactor designs do not require the period scram design feature because they are designed to accommodate rapid additions of reactivity). The log channel and a linear flux monitoring channel should accurately sense neutrons even in the presence of intense high gamma radiation.

Identify the maximum hypothetical accidents applicable to each mode of operation; this information should be consistent with the analysis provided in Chapter 13 of the SAR. Consideration should be given to failures that cause actions as well as prevent actions, such that all possible effects are examined. Further, failures that could lead to single or multiple rod position changes or out-of-sequence rod patterns should be analyzed. The staff considers operator error to be an anticipated operational occurrence, in addition to the consideration of single malfunction requirements, for which conformance to these requirements is to be evaluated.

Neutron flux (power) monitor channels covering the range from subcritical source multiplication to well beyond the licensed maximum power level.

Identify the variables that are monitored in order to provide protective action. The applicant/licensee's analysis, including the applicable portion provided in Chapter 13, should confirm that the system performance requirements are adequate to ensure completion of protective actions. The licensee should also identify the analytical limit associated with each variable. Performance requirements—including system response times, system accuracies, ranges, and rates of change of sensed variables to be accommodated until conclusion of the protective action—should also be identified in the system designation.

Separation between safety divisions begins with the sensors monitoring the variables and continues through the signal processing and actuation electronics. The licensee should describe the independence of the RPS detector or sensor devices for the reactor trip channels.

LSSSs are settings for automatic protective devices related to variables with significant safety functions. 10 CFR 50.36(c)(1)(ii)(A), “Technical Specifications,” requires that, where an LSSS is specified for a variable on which a safety limit has been placed, the setting be so chosen that automatic protective action will correct the abnormal situation before a safety level is exceeded.

Provide an analysis showing the establishment of the LSSS settings and describe how the settings will be verified.

RPS scram time as established in the accident analysis, and any other requirements to ensure operability.

The RPS scram time includes not only the rod drive speed both up and down and the time from scram initiation to the full insertion of any control rod from the full up position, but the system response time for initiating a scram.

Identify those variables that are monitored in order to provide protective action. Performance requirements -- including system response times, system accuracies, ranges, and rates of change of sensed variables to be accommodated until conclusion of the protective action -- should also be identified in the system designation. The applicant/licensee's analysis, including the applicable portion provided in Chapter 13, should confirm that the system performance requirements are adequate to ensure completion of protective actions.

Show that the the scram circuit is designed for the protective action to go to completion once it is initiated. Functional and logic diagrams can be provided to show that “seal-in” features are provided to enable system-level protective actions to go to completion. The circuit cannot be reset until all released rods are fully inserted.

The RPS shall always be capable of shutting down the reactor at least to the shutdown margin defined in the technical specifications.

A startup channel measuring neutrons at subcritical with a minimum count rate interlock to ensure operation and to prevent control or safety rod withdrawal unless the neutron count rate is at least some predetermined minimum such as 2 counts per second. This interlock may not be needed in reactor designs that use photoneutrons for startup. The applicant should justify not needing the interlock in this case. The detector is capable of detecting neutrons in a high gamma field and can be verified so that subcritical neutron multiplication can be determined and all reactivity changes can be monitored until the startup channel indication is overlapped by the log or linear channel power indication.

Where it is determined that the spatial dependence of a parameter requires several sensor channels to ensure the protection of the facility, the redundancy requirements are determined for the individual case. In certain designs, for example, adequate monitoring of core power requires a minimum number of sensors arranged in a given configuration to provide adequate protection. This aspect of redundancy is dealt with in coordination with the organization responsible for reviewing reactor designs to establish redundancy requirements.

Identify the number and location of those variables monitored to manually or automatically, or both, control each protective action that have a spatial dependence (that is, where the variable varies as a function of position in a particular region). The analysis should demonstrate that the number and location of sensors are adequate.

Redundant instrumentation sensing lines should be routed and protected so that any credible effects (consequences) of any design-basis event that is to be mitigated by signals sensed through those sensing lines should not render any of these redundant sensing lines inoperable unless it can be demonstrated that the protective function is still accomplished. This level of protection should ensure that after the event, a single failure should not prevent mitigation of that event. Credible effects of design-basis events that do not depend on a given group of redundant instrument-sensing lines for mitigation or accident prevention may render inoperable any or all of that group of sensing lines without violating this criterion. All nuclear safety-related instrument-sensing lines should be protected from damage during normal operational activities and occurrences.

Interlocks ensure that operator actions cannot defeat an automatic safety function during any operating condition where that safety function may be required. These interlocks include permissives for manually initiated operating bypasses and interlocks to ensure manually initiated operating bypasses are automatically removed when operating conditions would require the trip functions. Interlocks are also provided to ensure that manually initiated maintenance bypasses can only defeat a single train or channel of the RPS but not multiple channels or trains that would impair the system’s ability to function and meet the single-failure criteria.

Where operating requirements necessitate automatic or manual block of a protective function, the block is automatically removed whenever the appropriate permissive conditions are not met. Hardware and software used to achieve automatic removal of the block of a protective function are part of the RPS and, as such, are designed in accordance with the same criteria as the protective function.

Some operating bypasses may be automatically initiated when the permissive condition is sensed by the RPS input channel(s). An example of an automatically initiated operating bypass for the RPS would be automatically bypassing the high-source-range neutron flux trip by the power range neutron flux.

Some operating bypasses should be manually initiated. These operating bypasses can be manually initiated separately within each RPS division when the permissive condition is sensed by the RPS input channel(s). An example of a manually automatically initiated operating bypass for the RPS would be manually bypassing the high-source-range neutron flux trip with high-intermediate-range neutron flux.

All operating bypasses, either manually or automatically initiated, should be automatically removed when the facility moves to an operating regime where the protective action would be required if an accident occurred. Status indication should be provided in the MCR for all operating bypasses.

Provide a description of the permissive conditions for operating bypasses and the manual/automatic controls for those bypasses.

Equipment should meet its functional requirements during normal environmental conditions and anticipated operational occurrences, the requirements should be specified in the design/purchase specifications. A maintenance/surveillance program based on a vendor's recommendations, which may be supplemented with operating experience, should ensure that equipment meets the specified requirements.

For safety-related computer-based I&C systems, the evidence of qualification should be based on actual environmental conditions, and the records should be retained at a facility in an auditable and readily accessible form for review and use as necessary.

Provide a description of how the RPS equipment is designed to meet the functional performance requirements over the normal range of environmental conditions anticipated within the facility. The licensee should identify normal environmental conditions, including those resulting from anticipated operational occurrences, as applicable, for temperature, pressure, radiation, relative humidity, EMI/RFI, power surge environment, and operational cycling, and maximum hypothetical accidents to which the equipment is qualified.

The RPS should provide automatic initiation so that (1) fuel design limits are not exceeded and (2) accidents are sensed and mitigated. Both require timely operation of RPS components, thus establishing the timing requirements for detecting parameters exceeding their setpoints and equipment actuation in the RPS.

Specific timing requirements may affect system architecture because it may not be possible to get sufficient computational performance for a specific function or group of functions from a single processor, or the locations where functions are performed may be widely separated. Timing requirements may also increase complexity, either by fragmenting the system into multiple processors or by code tuning, which makes the software product harder to understand, verify, or maintain. The digital instrumentation loop often includes the sensor, transmitter, analog-to-digital converter, multiplexer, data communication equipment, demultiplexer, computers, memory devices, controls, and displays. Timing analysis should consider the entire loop.

The level of detail in the architectural description should include the number of message delays and computational delays interposed between the sensor and the actuator. An allocation of time delays to elements of the system and software architecture should be available. The digital instrumentation loop often includes the sensor, transmitter, analog-to-digital converter, multiplexer, data communication equipment, demultiplexer, computers, memory devices, controls, and displays. Timing analysis should consider the entire loop. In the initial design phases (e.g., at the point of design certification application), an estimated allocation of time delays to elements of the proposed architecture should be available. Subsequent detailed design and implementation should develop refined timing allocations down to unit levels in the software architecture.

A design should be feasible with currently known methods and representative equipment. Design timing feasibility may be demonstrated by allocating a timing budget to components of the system architecture so that the entire system meets its timing requirements. The timing budget should include internal and external communication delays, with adequate margins. Any non-deterministic delays should be noted and a basis provided that such delays are not part of any safety functions, nor can the delays impede any protective action.

Software architectural timing requirements should be addressed in a software architectural description. Databases, disk drives, printers, or other equipment or architectural elements subject to halting or failure should not be able to impede protective system action.

Provide an analysis of the real time performance of the RPS, from sensor to actuation.

A special concern for digital computer-based systems is confirmation that system real-time performance is adequate to ensure completion of protective action within the time scale derived from the applicable analyses in the SAR. The digital instrumentation loop often includes the sensor, transmitter, analog-to-digital converter, multiplexer, data communication equipment, demultiplexer, computers, memory devices, controls, and displays. Timing analysis should consider the entire loop. 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 design and implementation. Digital system architecture affects performance because communication between components of the system takes time, and allocation of functions to various system components affects timing. The architecture may also affect timing because an arrangement of otherwise simple components may have unexpected interactions.

The test should confirm operability of both the automatic and manual circuitry. When this capability can only be achieved by overlapping tests, the test scheme should be such that the tests do, in fact, overlap from one test segment to another. Test procedures that require disconnecting wires, installing jumpers, or other similar modifications of the installed equipment are not acceptable test procedures for use during power operation.

For digital computer-based systems, test provisions should address the increased potential for subtle system failures such as data errors and computer lockup.

Provide a description of the tests used to confirm performance of the RPS.

Design Criteria

Single Failure

An I&C system for a non-power reactor should be designed to perform its protective function after experiencing a single random active failure within the system.

Because digital computer-based I&C systems share data, data transmission, functions, and process equipment to a greater degree than analog systems, it can be more difficult to show that a single random failure or malfunction could not prevent the RPS from performing its intended function. Although this sharing forms the basis for many of the advantages of digital systems, it also raises a key concern with respect to I&C system vulnerability to a different type of failure. The concern is that a design using shared databases and process equipment has the potential to propagate a common-cause failure of redundant equipment. Another concern is that software programming errors can defeat the redundancy achieved by the hardware architectural structure. Because of these concerns, the NRC staff has placed significant emphasis on defense-in-depth against common-cause failures within and between functions. The principle of defense-in-depth is to provide several levels or echelons of defense to challenges to facility safety, such that failures in equipment and human errors will not result in an undue threat to public safety.

Any single failure within the safety (RPS) or nonsafety (RCS) system should not prevent proper protective action at the system level when required. Provide a description of the analysis used to confirm that the requirements of the single-failure criterion are satisfied.

Traditionally, diversity is used to protect against design inadequacies. If digital technology is used in the implementation, diversity should be considered to protect against implementation inadequacies.

Independent redundant or diverse reactor power level trips should be considered if a CCF failure of the RPS could result in exceeding the results in the accident analysis or have consequences within those of the MHA.

Assessments of adequate diversity in safety systems generally consider the following six attributes:

- design diversity,
- equipment diversity,
- functional diversity,
- human diversity,
- signal diversity, and
- software diversity.

As addressed in Section 7.2.1, the I&C systems should be designed to have functional reliability, including redundancy and diversity, commensurate with the safety functions to be performed and the consequences of failure of the system to perform the safety function. There should be at least two completely independent power level scram channels and they should provide diversity and redundancy. For example, the GA uses both the computer watchdog scram and the digital NM-1000 scram that provides diversity and redundancy to the scram system.

With the introduction of computers as a part of a safety system, concerns have arisen over the possibility that the use of computer software could result in a common-mode failure. Diversity is one method of addressing this concern.

The two principal factors for defense against common-cause failures (CCFs) are quality and diversity. Maintaining high quality will increase the reliability of both individual components and complete systems. Diversity in assigned functions (for both equipment and human activities), equipment, hardware, and software can reduce the consequences of a common-mode failure.

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.

Provide a description of the analysis that shows that vulnerabilities of the RPS to CCFs are adequately addressed. Where indicated by the SAR analysis as being necessary, a diverse means should be provided for initiating the affected RPS function or an alternate compensating function to mitigate the consequences of the identified design basis event for which action is required.

Independence

The RPS should be separated from control systems to the extent that failure of any single control system component or channel, or failure or removal from service of any single RPS component or channel which is common to the control and RPSs leaves intact a system satisfying all reliability, redundancy, and independence requirements of the RPS. Interconnection of the RPS and RCS systems should be limited so as to assure that safety is not significantly impaired.

To satisfy the requirements of independence, the safety system functions should maintain their independence between redundant portions of the safety system and between safety systems and other systems. The aspects of independence are:

- Physical independence.
- Electrical independence.
- Communications independence.

Physical independence can be achieved through physical separation (e.g., separate wireways, cable trays, and penetrations), or barriers (e.g., cabinets or rooms).

Electrical independence includes more than the use of separate power sources. To ensure electrical independence, fiber optic cables or qualified isolators can be used to interface all signals between equipment.

For digital interfaces, communications isolation is provided to ensure functional independence between systems. Communication isolation includes communication buffers, which provide separation between communication processing, functional processing, and functional logic, which ensures prioritization of all safety functions.

Communications independence should include confirmation that the routing of signals related to safety maintains (1) proper channeling through the communication systems, and (2) proper data isolation between redundant channels or alternatively, some form of data communication such that data from one channel cannot adversely affect to operation of another channel. Transmission of signals between independent channels should be through isolation devices.

Where data communication exists between different portions of a safety system, the licensee should confirm that a logical or software malfunction in one portion cannot affect the safety functions of the redundant portion(s). If a digital computer system used in a safety system is connected to a digital computer system used in a non-safety system, the licensee should confirm that a logical or software malfunction of the non-safety system cannot affect the functions of the safety system.

The I&C evaluation is limited to the review of components and electrical wiring inside racks, panels, and control boards for systems important to safety. The evaluation of the physical separation of electrical cables is addressed in the review of Chapter 8 of the SAR.

Provide a description of the physical, electrical, and communications independence of the RPS both within the RPS channels and between the RPS and non-safety-related systems. The description should be sufficient to show that the safety system design precludes the use of components that are common to redundant portions of the safety system, such as common switches for actuation, reset, mode, or test; common sensing lines; or any other features which could compromise the independence of redundant portions of the safety system. Physical independence is attained by physical separation and physical barriers.

The use of computers in safety systems has provided an opportunity for a high level of data communication between computers within a single safety channel, between safety channels, and between safety and non-safety computers. Improper use of this communication ability could result in the loss of a computer's ability to perform its function or multiple functions and thereby inhibit the safety system from performing its function.

Whenever communication techniques are employed, the major concern relates to the need to eliminate the potential loss of safety functions as a result of communication activities. This includes transmission of data and any vehicle for acknowledging receipt of the data or indicating a failure in data transmission. The detection and correction of any communication failures cannot be allowed to impede or interfere with the performance of safety functions. Communication faults should not adversely affect the performance of required safety functions in any way. Examples of credible communications include messages being corrupted because of errors in communications processors, errors introduced in buffer interfaces, errors introduced in the transmission media, or from interference or electrical noise; messages being repeated at an incorrect point in time; messages may be sent in the incorrect sequence, etc.

If the RPS and RCS are not part of a combined system, any data communication within a single safety channel, between safety channels, or between safety and non-safety systems should not inhibit the performance of the safety function. Isolation needs to be considered in order to prevent fault propagation between safety channels and from a non-safety computer to a safety computer. In practical terms, this means that for communications between safety and non-safety systems, the communications should be such that the safety system does not require any non-safety input to perform its safety function. In addition, any failure of the non-safety system, communications system, or data transmitted by the non-safety system should not prevent or influence the safety function of each safety channel. The portion of the safety software which actually performs the safety function, i.e., determining whether or not to trip based on sensor inputs, should not receive input or influence from any non-safety system while the safety system is on-line and performing that safety function.

If the safety and non-safety software reside on the same computer and use the same computer resources but are independent systems, either of the following approaches is acceptable to address the data communication issues:

- Barrier requirements should be identified to provide adequate confidence that the non-safety functions cannot interfere with performance of the safety functions of the software or firmware. The barriers should be designed in accordance with the requirements of the safety system software. The non-safety software is not required to meet these requirements.

- If barriers between the safety software and non-safety software are not implemented, the non-safety software functions should be developed in accordance with the requirements for safety system software.

For a combined RPS/RCS, the RCS should meet the requirements for the RPS. Equipment that is used for both safety and non-safety functions should be classified as part of the safety system. For this reason, any software providing non-safety functions that resides on a computer providing a safety function should be classified as a part of the safety system. If an applicant/licensee desires that a non-safety function be performed by a safety computer, the software to perform that function should be classified as safety-related, with all the attendant regulatory requirements for safety software, including communications isolation from other non-safety software.

Provide a description of data communications within and between safety channels and between safety and non-safety systems and how incoming and outgoing message data are stored and segregated. Provide a description of how the safety channels withstand communications faults and any barriers used to isolate systems and channels.

Protocols are standards and rules that allow computers to "talk" to each other—i.e., to send and receive messages over networks. Data communication protocol is a set of rules, formats, encodings, specifications, and conventions for transmitting data over a communication path. Typical safety communication protocols include Profibus between safety divisions and Ethernet between digital safety systems and safety human-machine interfaces (HMIs). Communications protocols are no different from any other software. That is, protocol design and protocol software should be treated with the same stringency as software in the safety subsystem the protocol serves.

Bandwidth is often used as a synonym for data transfer rate—the amount of data that can be carried from one point to another in a given time period (usually a second). A channel with x bps may not necessarily transmit data at x rate, because protocols, encryption, and other factors can add appreciable overhead. In fact, the proximate cause of performance failure in digital communications systems is that actual data rates exceed the capabilities of one or more data links, or the ability of associated nodes to handle the traffic. A node should also have sufficient computational capacity left after handling communication traffic to perform its other functions.

For the protocols used in the RPS, the licensee should discuss actual protocol functions needed to perform the safety mission should be determined. At a minimum, safety, liveness, and real-time performance properties required by the safety application should be verified in the protocol. Safety properties describe what a system is allowed to do. Liveness properties describe what it should do. Real-time performance properties describe how quickly it should do its job to meet externally imposed system deadlines. The use of the services provided by the protocol by the safety application should be reviewed for appropriateness. Inefficiency, unused services, or excessive application software complexity when using protocol services are indications that the chosen protocol does not match the safety requirements well.

Data rates, data bandwidths, and data precision requirements for normal and off-normal operation, including the impact of environmental extremes, should be discussed by the licensee. There should be sufficient excess capacity margins to accommodate likely future increases in data communication demands or software or hardware changes to equipment attached to the data communication system. The error performance should be specified. Vendor test data and in situ test results should be reviewed to verify the performance. Analytical justifications of data communication systems capacity should be reviewed for correctness. The interfaces with other data communication systems or other parts of the I&C system should be reviewed to verify compatibility.

Equipment Qualification

Show that the RPS is designed for reliable operation in the normal range of environmental conditions anticipated within the facility. If environmental controls such as heat tracing of instrument lines or cabinet cooling fans are necessary to protect equipment from environmental conditions, these should also be described.

Electromagnetic interference (EMI), radio-frequency interference (RFI), and power surges have been identified as environmental conditions that can affect the performance of safety-related electrical equipment.

Fiber optics typically offer resistance to such effects but have other attributes that prevent universal acceptability. For example, if the fiber-optic medium may be subject to radiation, fiber that does not become opaque or brittle under irradiation should be specified, or there should be a defined replacement schedule.

Provide a description of the design, installation, and testing practices for addressing the effects of EMI/RFI and power surges on safety-related instrumentation and control (I&C) systems. Information should be sufficient to allow a reviewer to confirm that data communication media do not present a fault propagation path for environmental effects, such as high-energy electrical faults or lightning, from one redundant portion of a system to another or from another system to a safety system.

Prioritization of functions

A priority function receives device actuation commands from safety and non-safety sources, and sends the command having highest priority to one or more safety-related actuated devices. The actuated device is a safety-related component such as a motor actuated valve, a pump motor, a solenoid operated valve, etc. The priority module should also be safety-related.

Safety-related commands that direct a component to a safe state should always have the highest priority and should override all other commands. Communication isolation for each priority module should be as described in the guidance for interdivisional communications. Software-based prioritization should meet all requirements (quality requirements, V&V,

documentation, etc.) applicable to safety-related software. To minimize the probability of failures because of common software, the priority module design should be fully tested. (This refers to proof-of-design testing, not to individual testing of each module and not to surveillance testing.) Automatic testing within a priority module, whether initiated from within the module or triggered from outside, and including failure of automatic testing features, should not inhibit the safety function of the module in any way. The priority module should ensure that the completion of a protective action is not interrupted by commands, conditions, or failures outside the module's own safety division.

Provide a description of the priority functions within the RPS and the proof-of-design tests to verify that it meets its intent as specified. Provide a description of the selection of a particular command to send to an actuator when multiple and conflicting commands exist.

Setpoints

For setpoints that have a significant importance to safety, a rigorous setpoint methodology should be used. The methodologies utilized should be documented and appropriate justification for their use should be provided.

Because all measurements are imperfect attempts to ascertain an exact natural condition, the actual magnitude of the quantity can never be known. Therefore, the actual value of the error in the measurement of a quantity is also unknown. There are a number of recognized methods for combining instrumentation uncertainties such as the statistical square root sum of squares (SRSS) methods to combine random uncertainties and then algebraically combine the nonrandom terms with the result.

Provide a description of the methodology used to determine the setpoints for the RPS, including a description of the uncertainties associated with the parameters used.

For both direct and indirect parameters, the applicant/licensee should show that the characteristics (e.g., range, accuracy, resolution, and response time) of the instruments that produce the RPS inputs are consistent with the analysis.

Show that any indirect parameter is a valid representation of the desired direct parameter for all events.

10 CFR 50.36(c)(1)(ii)(A), "Technical Specifications," requires that, where a LSSS is specified for a variable on which a safety limit has been placed, the setting be so chosen that automatic protective action will correct the abnormal situation before a safety level is exceeded. LSSSs are settings for automatic protective devices related to variables with significant safety functions. Setpoints found to exceed technical specification limits are considered as malfunctions of an automatic safety system. Such an occurrence could challenge the integrity of the reactor core, reactor coolant pressure boundary, containment, and associated systems.

Accident analyses establish the limits for critical process parameters. These analytical limits, as established by accident analyses, do not normally include considerations for the accuracy (uncertainty) of installed instrumentation. Additional analyses and procedures are necessary to assure that the limiting trip setpoint of each safety control function is appropriate.

Provide a description of the physical features of the RPS that assure that the proper setpoints are automatically made active or include features that facilitate administrative controls to verify the proper setpoints, or both, when the operating mode of the reactor is changed.

Operational Bypass/Permissives and Interlocks

Any individual channels for which bypassing is allowed during reactor operation should be justified in the SAR. Only minimal bypassing should be permitted in safety systems and never in a system that could compromise scram capability of the other channels.

The purpose of interlocks is to maintain the RPS in a state that assures its availability in an accident. For the I&C systems, interlocks are used to isolate safety systems from non-safety systems, and interlocks to preclude inadvertent inter-ties between redundant or diverse safety systems where such inter-ties exist for the purposes of testing or maintenance.

The requirement for automatic removal of operational bypasses means that the reactor operator should have no role in such removal. The operator may take action to prevent the unnecessary initiation of a protective action.

Whenever the applicable permissive conditions are not met, a safety system feature that physically prevents or facilitates administrative controls to prevent unauthorized use of bypasses. If operating conditions change so that an activated operating bypass is no longer permissible, the safety system should automatically accomplish one of the following actions:

- Remove the appropriate active operating bypass(es).
- Restore conditions so that permissive conditions once again exist.
- Initiate the appropriate safety function(s).

The requirement for automatic removal of operational bypasses means that the reactor operator should have no role in such removal. The operator may take action to prevent the unnecessary initiation of a protective action.

Provide a description of the interlocks within the RPS, the conditions for their initiation and removal, and which conditions are manual, automatic, or both.

At times, administrative procedures may allow safety functions to be bypassed or made inoperable during the performance of periodic tests or maintenance. These procedures should be supplemented by an indication system that automatically indicates, for each affected safety system or subsystem, the bypass or deliberately induced inoperability of a safety function and the systems actuated or controlled by the safety function. Provisions should also be made to allow the operations staff to confirm that a bypassed safety function has been properly returned to service.

If a facility's administrative procedures may require that the operator give permission before the initiation of any activity that would or could affect a safety system, the decision to grant such permission should be based on knowledge of the operating status of the safety systems, the extent to which the activity will affect those systems, and whether that effect is permissible within the provisions of the license. However, when the measures used to indicate inoperable status consist solely of administrative procedures, the operator may not always be fully aware of the ramifications of each bypassed or inoperable component.

If the protective action of some part of the RPS is bypassed or deliberately rendered inoperative for testing, that fact should be continuously indicated in the control room. Operations staff should also be able to confirm that a bypassed safety system has been properly returned to service.

Provide a list of those safety functions that can be administratively bypassed and discuss measures to inform the operators of its status.

In most cases, bypasses of a part of the RPS to perform periodic testing during reactor operation should be allowed only when the remainder of the RPS satisfies the single-failure criterion. However, exceptions to the single-failure criterion include, if supported by its safety analysis, negligible-risk research reactors or pulse-reactors. In addition, a probabilistic assessment of the RPS may be used to eliminate certain postulated failures from consideration on the basis that such failures are shown not to be credible. If trustworthy failure rate data are available, reliability analysis may be used to demonstrate that the RPS satisfies such sufficient reliability goals that allows exemption from the single-failure criterion.

For those facilities where the single-failure criterion is applicable to the design of the RPS, additional redundancy should be provided to the extent necessary to assure that loss of protective action at the system level is not credible in those instances where a credible single failure could both initiate an event and cause the loss of the corresponding protective action. Nevertheless, for one-out-of-two portions of the RPS, compliance with the single-failure criterion may not be mandatory when a bypass is necessary for a brief time to perform periodic testing if the reliability of the portion remaining active has been shown to be acceptable. For example, if the time permitted for the bypass has been shown to be so brief that the probability that the active portion might fail during the bypass time is commensurate with the probability that the one-out-of-two system might fail during the normal operating time between tests.

The licensee should discuss the capability of the RPS to accomplish its safety function while execute features equipment is in maintenance bypass. If an exemption from the single-failure criterion is maintained, the licensee should provide a reliability analysis used to demonstrate that reliability goals are met.

Isolation devices are used to assure that credible failures in the connected non-safety or redundant channels will not prevent the safety systems from meeting their required functions. Isolation devices between the safety system and a non-safety system are classified as part of the safety system.

In most facilities, the RPS will include separation and isolation methods adequate to protect each interface with non-RPS equipment. In those cases where the software for the safety and non-safety systems reside on the same computer and use the same computer resources, the licensee should provide the following information:

- Identification of any barriers, such as broadcast communication or buffering circuits for communications isolation, and fiber optic cable or optical isolators for electrical isolation, used to provide adequate confidence that the non-safety functions cannot interfere with performance of the safety functions of the software or firmware.

- If barriers between the safety software and non-safety software are not implemented, the non-safety software functions were developed in accordance with the requirements of a safety system.

Provide a description of the barriers and isolation devices/techniques used to isolate the safety-related RPS from the non-safety-related I&C systems.

Electrical power circuits should be isolated sufficiently to avoid electromagnetic interference with safety-related instrumentation and control functions. This is reviewed in Section 8.1 of NUREG-1537.

Surveillance

If continuity of operation is a requirement, then the RPS should be designed to permit periodic testing of its functioning when the reactor is in operation, including a capability to test channels independently to determine failures that may have occurred. Where safety system testing during operation of the RTR is required or provided as an option, the RPS design should retain the capability to accomplish its safety function while under test.

To maintain reliable and accurate performance, I&C systems undergo testing and calibration. Calibration, especially in analog systems, is used to address instrument drift, inaccuracies, and errors. The performance of analog systems can typically be predicted by the use of engineering models. Inspection and testing are used to verify correct implementation and to validate desired functionality of the final product, in both analog and digital systems.

One benefit of digital I&C systems is the use of self-testing, which is a test or series of tests performed by a device upon itself. Self-tests include on-line continuous self-diagnostics, equipment-initiated self-diagnostics, and operator-initiated self-diagnostics. Self-testing can be used for the early identification of inoperable equipment. When self-diagnostics are applied, the following self-diagnostic features should be incorporated into the system design: Self-diagnostics during computer system startup, periodic self-diagnostics while the computer system is operating, and self-diagnostic test failure reporting.

Test and calibration functions should not adversely affect the ability of the computer to perform its safety function. V&V, configuration management, and QA should be required for test and calibration functions on separate computers (e.g., test and calibration computer) that provide the sole verification of test and calibration data. V&V, configuration management, and QA should be required when the test and calibration function is inherent to the computer that is part of the safety system.

Surveillance tests are conducted to confirm compliance operability of the system.

Provide a summary of the calibration, inspection, and testing (including self-tests and surveillance tests) to confirm operability of the desired functionality of the RPS.

10 CFR 50.36(c)(3), “Technical Specifications,” states that surveillance requirements are 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. Maintaining system performance provides

the basis for the technical specifications of non-power reactors (Ch. 14), consistent with the safety analysis with respect to reliability, availability, and capability of the RPS.

Provide a summary of its technical specifications and the bases for the surveillance intervals used in its safety analyses.

Classification and Identification

In order to provide assurance that the design, construction, maintenance, and operation of the facility meet the design criteria, the licensee should describe the following:

- How safety system equipment should be identified for each redundant portion of a safety system,
- How the identification of safety system equipment is distinguishable from any identifying markings placed on equipment for other purposes (for example, identification of fire protection equipment, phase identification of power cables).

One acceptable method of identification is color coding of components, cables, and cabinets.

Provide a description of how the safety system equipment is identified for each redundant portion of a safety system and how the identification of safety system equipment is distinguishable from any identifying markings placed on equipment for other purposes.

Human Factors

Human factors engineering principles and criteria should be applied to the selection and design of the displays and controls. Human-performance requirements should be described and related to the facility's safety criteria. Recognized human-factors standards and design techniques should be employed to support the described human-performance requirements.

Provide a summary of the human-machine interface principles used in the location of instrumentation and controls for the RPS.

The RPS should include means for manual initiation of each protective action at the system level (e.g., reactor trip). The control interfaces for manual initiation of protective actions should be easily accessible to the operator so that action can be taken in an expeditious manner at the point in time or under the facility's conditions for which the protective actions of the safety system should be initiated. Information displays associated with manual controls should (i) be readily present during the time that manual actuation is necessary, (ii) be visible from the location of the manual controls, and (iii) provide unambiguous indications that will not confuse the operator.

The location of manual controls should incorporate human factors to ensure that the functions controlled and the characteristics of the controls (e.g., location, range, type, and resolution) allow operators to take appropriate manual actions.

The manual scram switch is located where the operator has ready access, such as near the rod drive controls.

The information displayed and the characteristics of the displays (e.g., location, range, type, and resolution) support operator awareness of system and facility's status and will allow facility's operators to make appropriate decisions.

The annunciator system is considered to consist of sets of alarms (which may be displayed on tiles, video display units [VDUs], or other devices) and sound equipment; logic and processing support; and functions to enable operators to silence, acknowledge, reset, and test alarms. The main control room (MCR) should contain compact, redundant operator workstations with multiple display and control devices that provide organized, hierarchical access to alarms, displays, and controls. Each workstation should have the full capability to perform MCR functions as well as support division of tasks between two operators.

The designer should use existing defensive measures (e.g., segmentation, fault tolerance, signal validation, self-testing, error checking, supervisory watchdog programs), as appropriate, to assure that alarm, display, and control functions provided by the redundant workstations meet these criteria. Alarms that are provided for manually controlled actions for which no automatic control is provided, and that are required for the safety systems to accomplish their safety functions, should meet the applicable specifications for Class 1E equipment and circuits.

Upon receipt of a scram signal, the RPS will annunciate the scram and signify the circuits that are in a tripped state.

Quality

For construction permits, 10CFR50.55a(a)(1) requires that structures, systems, and components be designed, fabricated, erected, constructed, tested, and inspected to quality standards commensurate with the importance of the safety function to be performed. Licensee's should consider these requirements for operations and maintenance.

The quality standards and design control measures for the RPS should be provided for verifying or checking the adequacy of design. 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.

Provide a description of design criteria for the RPS and a statement that the criteria and guidelines for implementing those criteria will be implemented in the design of RPS.

Managerial and administrative controls can be part of the quality assurance used to assure safe operation. 10 CFR 50.34(a)(7) requires that applicants for construction permits describe a quality assurance program for the design and construction of the structures, systems, and components of the facility. 10 CFR 50.34(b)(6)(ii) requires a description in the SAR of managerial and administrative controls to be used to ensure safe operation. ANSI/ANS 15.8-1995, endorsed by RG 2.5, provides an acceptable method in developing a quality assurance program for the design, construction, testing, modification, and maintenance of research and test reactors for complying with the program requirements of 10 CFR 50.34.

Provide a description of the overall quality assurance program requirements. he program should identify the items and activities to which it applies and the extent of program application for each item and activity. The program should provide for the appropriate and necessary indoctrination and training of personnel who perform activities that affect quality, to ensure that suitable proficiency is achieved and maintained.

Use of Digital Systems

Software development plans can be used to provide a high-quality software life cycle process. These plans commit to documentation of life cycle activities that enhance the quality of the design features upon which the safety determination is based.

Digital I&C systems are fundamentally different from analog I&C systems. Digital I&C systems can share code, data transmission, data, and process equipment to a greater degree than analog systems. Minor errors in design and implementation can cause them to exhibit unexpected behavior. Consequently, the performance of digital systems over the entire range of input conditions cannot generally be inferred from testing at a sample of input conditions. Inspections, type testing, and acceptance testing of digital systems and components do not alone accomplish design qualification at high confidence levels. To address this issue, the design qualification for digital systems focuses to a large extent on the applicant/licensee employing a high-quality development process that incorporates disciplined specification and implementation of design requirements. Inspection and testing are used to verify correct implementation and to validate desired functionality of the final product, but confidence that isolated, discontinuous point failures will not occur derives from the discipline of the development process.

The development of safety system software should progress according to a formally defined life cycle (e.g., Concepts; Requirements; Design; Implementation; Test; Installation, Checkout, and Acceptance Testing; Operation; Maintenance; Retirement). The software developer should select and document the software life cycle, and specify the products that will be produced by that life cycle. The software developer can be the applicant/licensee, the vendor, a company working on behalf of either, or a commercial software development company.

Although not required, specific output documents that formally document the development process and are helpful in also documenting the successful completion/planning throughout the life cycle processes. The information to be reviewed may be contained in the following documents:

- Software Management Plan (SMP).
- Software Development Plan (SDP).
- Software Quality Assurance Plan (SQAP).
- Software Integration Plan (SIntP).
- Software Installation Plan (SInstP).
- Software Maintenance Plan (SMaintP).
- Software Training Plan (STrngP).
- Software Operations Plan (SOP).

- Software Safety Plan (SSP).
- Software Verification and Validation Plan (SVVP).
- Software Configuration Management Plan (SCMP).
- Software Test Plan (STP).

Provide a description of the software development activities. If the software or system development was delegated to others, the authority, duties, verifying, and any activities that can affect the safety-related functions should be discussed.

Verification and validation (V&V) and Independent verification and validation (IV&V) are used to verify that implementation of the software life cycle process meets the criteria expected for high-quality software.

V&V processes provide an objective assessment of software products and processes throughout the software life cycle. his assessment demonstrates whether the system requirements and software requirements (i.e., those allotted to software via software specifications) are correct, complete, accurate, consistent, and testable. These V&V processes are used to determine whether the development products of an activity conform to the requirements of that activity, and whether the system performs according to its intended use and user needs. This determination of suitability includes assessment, analysis, evaluation, review, inspection, and testing of products and processes.

The levels of independence required for the V&V effort are defined by three parameters: technical independence, managerial independence, and financial independence.

The V&V activities and tasks should include system testing of the final integrated hardware, software, firm-ware, and interfaces. The V&V effort should be allocated resources that are independent of the development resources.

The table below provides V&V tasks, inputs, and outputs for each life cycle process (e.g., management, acquisition, supply, development, operation, maintenance) that should be addressed:

V&V Activity
Component V&V test plan and test procedure generation
Concept documentation evaluation
Criticality analysis
Software hazard analysis
Installation checkout
Identify improvement opportunities in the conduct of V&V

Integration V&V test case, design, execution, plan, and procedure generation

Interface analysis

Management review of the V&V effort

New constraints evaluation

Planning the interface between the V&V effort and supplier

Proposed/baseline change assessment

Scoping the V&V effort

Security analysis

Software design and requirements evaluations

Software V&V plan generation and revision

Source code and source code documentation evaluation

System requirements review

System V&V test case, design, execution, plan, and procedure generation

Task iteration

Traceability analysis

V&V final report generation

The development activities and tests should be verified and validated by individuals or groups with appropriate technical competence, other than those who developed the original design. Oversight of the IV&V effort should be vested in an organization separate from the development and program management organizations.

Provide a description of the V&V processes for the computer hardware and software, the integration of the digital system components, and the interaction of the resulting computer system with the nuclear facility. The V&V activities and tasks should include system testing of the final integrated hardware, software, firm-ware, and interfaces.

Configuration management (CM) is a significant part of high quality engineering activities. The quality assurance criteria for software is implemented through a configuration management program, which includes criteria for administrative control, design documentation, design interface control, design change control, document control, identification and control of parts and components, and control and retrieval of qualification information associated with parts and components.

While the principles and intentions of traditional configuration management apply equally to software, with software there is a greater emphasis on the design process; the deliverable product is more like a design output. With engineered software, a large amount of the design process information and many intermediate design outputs are associated with the final design output. Relatively many software engineering changes are expected and encountered. Consequently, although similar in intent to hardware configuration management, software configuration management requires a change in emphasis, with expansion of the importance of intermediate design baselines and associated design process information. The needs for robust change management and identification and control of product versions are also substantially increased.

Software changes should be traced to their point of origin, and the software processes affected by the change should be repeated from the point of change to the point of discovery. Proposed changes should be reviewed for their impact on system safety. Status accounting should take place for each set of life cycle activities prior to the completion of those activities. The status accounting should document configuration item identifications, baselines, problem report status, change history and release status.

Provide a description of the following set of activities associated with configuration management of its safety system software:

a. Identification and control of all software designs and code,

b. Identification and control of all software design functional data (e.g., data templates and data bases),

c. Identification and control of all software design interfaces,

d. Control of all software design changes,

e. Control of software documentation (user, operating, and maintenance documentation),

f. Control of software vendor development activities for the supplied safety system software,

g. Control and retrieval of qualification information associated with software designs and code,

h. Software configuration audits, and

i. Status accounting.

Software risk management can be used for identifying potential problems, assessing their impact, and determining which potential problems should be addressed to assure that software quality goals are achieved.

Software project risks may include technical, schedule, or resource-related risks that could compromise software quality goals, and thereby affect the ability of the safety computer system to perform safety-related functions. Risk factors include system risks, mechanical/electrical hardware integration, risks due to size and complexity of the product, the use of pre-developed software, cost and schedule, technological risk, and risks from program interfaces (maintenance, user, associate contractors, subcontractors, etc.).

Risk management should include the following items:

i. Determine the scope of risk management to be performed for the digital system

ii. Define and implement appropriate risk management strategies

iii. Identify risks to the software project in the project risk management strategy and as they develop during the conduct of the project

iv. Analyze risks to determine the priority for their mitigation

v. Develop risk mitigation plans for risks that have the potential to significantly impact software quality goals, with appropriate metrics for tracking resolution progress. (These risks may include technical, schedule, or resource-related project risks that could compromise the ability of the safety computer system to perform safety related functions)

vi. Take corrective actions when expected quality is not achieved

vii. Establish a project environment that supports effective communications between individuals and groups for the resolution of software project risks.

Software project risk management differs from hazard analysis. A hazard is a condition that is prerequisite to an accident. Hazards include external events as well as conditions internal to computer hardware or software. The software and hardware safety plan addresses the identification, evaluation and resolution of hazards. Hazard analysis is the process that explores and identifies conditions that are not identified by the normal design review and testing process. The scope of hazard analysis extends beyond plant design basis events by including abnormal events and plant operations with degraded equipment and plant systems. The software safety plan should include the safety analysis implementation tasks that are to be carried out by the applicant/licensee. The acceptance criterion for software safety analysis implementation is that the tasks in that plan have been carried out in their entirety.

Provide a description of the method to be used to ensure that hazards which software is expected to control are resolved in an acceptable manner. The description should include a requirement that a safety analysis be performed and documented on each of the principal design documents: requirements, design descriptions, and source code. Hazards, including abnormal events and conditions and malicious modifications, should be analyzed and documented. Hazard reduction efforts should be documented.

A set of indicators could be used to determine the success or failure of the software safety effort. The systematic collection and analyses of software safety data could then be used to determine the effectiveness of the software safety effort.

Software testing consists of testing the smallest testable units, and then integrating those units into larger testable units, and testing as an integrated unit. This process is repeated until finally the system is tested after installation.

Testing should be performed with the computer functioning with the software and diagnostics that is representative of those used in actual operation. All portions of the computer necessary to accomplish safety functions, or those portions whose operation or failure could impair safety functions, should be exercised during testing. This includes, as appropriate, exercising and monitoring the memory, the central processing unit, inputs, outputs, display functions, diagnostics, associated components, communication paths, and interfaces. Testing should demonstrate that the performance criteria related to safety functions have been met.

In those cases in which traditional qualification processes cannot be applied, an alternative approach to verify that a component is acceptable for use in a safety-related application is commercial grade dedication. The objective of commercial grade dedication is to verify that the item being dedicated is equivalent in quality to equipment developed under the licensees QA program. The dedication process for the computer should entail identification of the physical, performance, and development process requirements necessary to provide adequate confidence that the proposed digital system or component can achieve the safety function. The dedication process should apply to the computer hardware, software, and firmware that are required to accomplish the safety function. The dedication process for software and firmware should include an evaluation of the design process.

Provide a description of the following set of activities for the safety system software:

- test planning, which consists of a test plan that addresses key aspects of the test program, such as scope, risks, tasks, resources, responsibilities, and acceptance (pass or fail) criteria for the software item being tested.

- test specification, which consists of test designs, test cases, and test procedures that contain the detailed procedures and instructions for testing as well as the feature or test case acceptance criteria to be employed during the testing effort should be provided, and

- test reporting, which consists of transmittal reports, test incident reports, test logs, and test summary reports that provide for the recording and summarization of test events and that serve as the basis for evaluating test results. All information in this category is summarized in the test summary report.

Software requirements specification is an essential part of the record of the design of safety system software and serves as the design bases for the software to be developed. Correct, complete, well-written and unambiguous software requirements are essential inputs to the design and verification processes that are necessary to produce high-integrity software products. Therefore, software requirements specifications are a crucial design input to the software development process.

The software requirements specifications will facilitate the implementation of a carefully planned and controlled software development process. The software requirements specifications for the safety system software should include at a minimum a description of every input (stimulus) into the system, every output (response) from the system, and all functions performed by the system in response to an input or in support of an output. A software requirements specification that exhibits the functional and the software development process characteristics listed below should be produced.

Functional Characteristics of software requirements specification include:

- **Accuracy** requirements should be stated numerically, and appropriate physical units and error bounds should be supplied.

- **Functionality** means that functions should be specified in terms of inputs to the function, transformations to be carried out by the function, and outputs generated by the function.

- **Reliability** means that all requirements for fault tolerance and failure modes are fully specified for each operating mode.

- **Robustness** means that the behavior of the software in the presence of unexpected, incorrect, anomalous and improper (1) input, (2) hardware behavior, or (3) software behavior is fully specified.

- **Safety** means that the software functions, operating procedures, input, and output be classified according to their importance to safety and should be identified as such in the SRS.

- **Security** means that security threats to the computer system are identified and classified according to severity and likelihood. Actions required of the software to detect, prevent, or mitigate such security threats should be specified, including access control restrictions.

- **Timing** means that functions that should operate within specific timing constraints are identified, and that timing criteria are specified for each. Timing requirements should distinguish between goals and requirements.

Process Characteristics of software requirements specification include:

- **Completeness** means that all actions required of the computer system are fully described for all operating modes and all possible values of input variables. The software requirements specification should also describe any actions that the software is prohibited from executing.

- **Consistency** means that the contents of the software requirements specification are consistent with the safety system requirements, the safety system design, and documented descriptions and known properties of the operational environment within which the safety system software will operate.

- **Correctness** means that the description of actions required of the computer system are free from faults and that no other requirements are stated.

- **Style** means that the contents of the software requirements specification are understandable. The software requirements specification should differentiate between requirements placed on the software and other supplementary information, such as design constraints, hardware platforms, and coding standards.

- **Traceability** means that a two-way trace exists between each requirement in the software requirements specification and the safety system requirements and design. There should be a two-way trace between each requirement in the software requirements specification and the software design, as well as a forward trace from each requirement in the software requirements specification to the specific inspections, analyses, or tests used to confirm that the requirement has been met.

- **Unambiguity** means that each requirement, and all requirements taken together, have one and only one interpretation.

- **Verifiability** means that it is possible to construct a specific analysis, review, or test to determine whether each requirement has been met.

Errors in requirements or misunderstanding of requirements intent are major sources of software errors. Each of the above functional characteristics should be present in each requirement. If the requirements are not clearly stated, they will probably not be clear to the software design team.

Provide a description of the method for achieving high functional reliability and design quality in the software used in the safety systems. Each requirement should be complete, consistent with the overall safety system requirements, and not in conflict with some other requirement. The requirements should be understandable and unambiguous. Each requirement should be traceable to one or more safety system requirements, and a requirements traceability matrix could be used to show where in the software the required action is being performed. A requirements traceability matrix would also show where the particular requirement is being tested.

Because there is not a widely accepted view on software reliability value, determining a failure probability, and therefore a reliability value, is not possible. There is no industry consensus on a method to quantify software reliability and/or availability. Highly reliable software relies very heavily on the software development process to ensure reliable software because testing cannot cover all possible conditions that the software may encounter in actual service.

Quantitative reliability determination, using a combination of analysis, testing, and operating experience, can provide an added level of confidence in the reliable performance of the computer system. When reliability goals are identified, the proof of meeting the goals should include the software. The method for determining reliability may include combinations of analysis, field experience, or testing. Reliability of software might be demonstrated by evaluation of the development process combined with testing under a wide range of input conditions. Software error recording and trending may be used in combination with analysis, field experience, or testing. Compensation for the deficiencies in original development process needs to be thorough and systematic to provide confidence that the software will perform its safety function when needed. The qualification method should not rely heavily on operating history for a system that is intended to protect with extraordinarily high reliability against low-frequency events. The normal facility's operating history is not particularly likely to generate unusual and rare conditions that were not anticipated and which are the cause of a software malfunction.

Provide a description of the software reliability measures and the means for attaining software reliability goals.

Access Control

Physical and electronic access to digital computer-based control system software and data should be controlled to prevent changes by unauthorized personnel. Control should address access via network connections and via maintenance equipment.

Access control uses design features to provide the means to control physical access to safety system equipment, including access to test points and means for changing setpoints. Typically such access control includes provisions such as alarms and locks on safety system panel doors, or control of access to rooms in which safety system equipment is located. Thus, all safety-related digital components and network cabling should be installed in a facility's location that physically secures the equipment. Portable computer equipment intended to interface with the safety-related equipment should not be used for other purposes, and should not be taken out of and returned to the protected area without appropriate controls and safeguards.

Controls used to prevent unauthorized access should address access via network connections, and via maintenance equipment. All remote access should be prohibited. Remote access is defined by the safety system's computer security assessment. Wireless connectivity should not be implemented. All wireless capabilities should be disabled on workstations. All wireless capabilities on maintenance and test equipment should be disabled prior to connecting to safety-related equipment.

Provide a description of those provisions to prevent unauthorized access to hardware and software, throughout the life cycle, for the RPS.

To provide assurance that the required computer system hardware and software are installed in the appropriate system configuration, the following identification requirements specific to software systems should be met:

i. Firmware and software identification should be used to assure the correct software is installed in the correct hardware component.

ii. Means should be included in the software such that the identification may be retrieved from the firmware using software maintenance tools.

iii. Color coding of components, cables, and cabinets can be used to provide physical identification of the digital computer system hardware.

iv. The identification should be clear and unambiguous. The identification should include the revision level, and should be traceable to configuration control documentation which identifies the changes made by that revision.

Provide a description of any program used to ensure that the correct version of the software/firmware is installed in the correct hardware components.

Cyber Security

Computer-based systems are secure from electronic vulnerabilities if unauthorized and inappropriate access and use of those systems is deterred, detected, and mitigated. The security of computer-based systems is established through (1) designing the security features that will meet licensee's security requirements in the systems, (2) developing the systems that do not contain undocumented codes (e.g., back door coding, logic, and/or time bomb codes) and that are resilient to malicious programs (e.g., viruses, worms, and Trojan horses), and (3) installing and maintaining those systems in accordance with the station administrative procedures and the licensee's security program.

Licensees should provide high assurance that digital computer and communication systems and networks are adequately protected against cyber attacks, up to and including the maximum hypothetical accident, from internal and external threats. Licensees should protect from cyber attacks digital computer and communication systems associated with certain categories of functions and support systems and equipment, which, if compromised, would adversely impact the safety-related and important-to-safety functions, security functions, and emergency preparedness functions (including offsite communications) at the facility.

The licensee should:

1. Establish, implement, and maintain a cyber security program for software that provides a protection system function; and

2. Incorporate the cyber security program as a component of the physical protection program.

The cyber security program should be designed to:

1. Implement security controls to protect the RPS from cyber attacks;

2. Apply and maintain defense-in-depth protective strategies to ensure the capability to detect, respond to, and recover from cyber attacks;

3. Mitigate the adverse affects of cyber attacks; and

4. Ensure that the functions of the RPS are not adversely impacted due to cyber attacks.

As part of the cyber security program, the licensee should:

1. Ensure that appropriate facility personnel, including contractors, are aware of cyber security requirements and receive the training necessary to perform their assigned duties and responsibilities.

2. Evaluate and manage cyber risks.

3. Ensure that modifications to safety system software or hardware, are evaluated before implementation to ensure that the cyber security performance objectives are maintained.

The licensee should establish, implement, and maintain a cyber security plan that implements the cyber security program requirements of the RPS.

1. The cyber security plan should describe how the requirements of this section will be implemented and should account for the site-specific conditions that affect implementation.

2. The cyber security plan should include measures for incident response and recovery for cyber attacks. The cyber security plan should describe how the licensee will:

   i. Maintain the capability for timely detection and response to cyber attacks;

   ii. Mitigate the consequences of cyber attacks;

   iii. Correct exploited vulnerabilities; and

   iv. Restore affected systems, networks, and/or equipment affected by cyber attacks.

The licensee should develop and maintain written policies and implementing procedures to implement the cyber security plan. Policies, implementing procedures, site-specific analysis, and other supporting technical information used by the licensee need not be submitted for Commission review and approval as part of the cyber security plan but are subject to inspection by NRC staff on a periodic basis.

The licensee should review the cyber security program as a component of the physical security program, including the periodicity requirements.

The licensee should retain all records and supporting technical documentation for at least three (3) years after the record is superseded.

- The applicant should discuss the conclusions about capability, operability, and suitability of the RPS requested in **Section 7.2.5.** That is, the applicant should summarize in this section of the SAR why the system design is sufficient and suitable for performing the functions stated in the design bases.

7.5 Engineered Safety Features Actuation Systems

If ESFs are required by the accident analyses in Chapter 13, their actuation systems should be described in this section. The ESF actuation system senses the need for and initiates the operation of ESF systems (1) to prevent or mitigate the consequences of damage to fission product barriers such as fuel, cladding, or fueled experiments caused by overpower or loss-of-cooling events or (2) to gain control of any radioactive material released by accidents.

Each active ESF should be automatically initiated by a subsystem of the ESF actuation system. Examples of such systems include those to actuate an active emergency core cooling system (ECCS), containment or confinement system, containment or confinement air cleanup and filtration system, or any other ESF that is designed to perform a mitigative function. Most non-power reactors do not have an active ECCS because they are designed to rely on passive ECCS or natural coolant circulation to provide sufficient core cooling to prevent loss of fuel integrity. Certain non-power reactors may not be required by the accident analyses to have containment or confinement ESF systems or a containment or confinement air cleanup and filtration ESF system. When such systems are required, their actuation systems should be described in this section, in coordination with the information in Chapter 6, "Engineered Safety Features," of the SAR.

Certain parameters should be monitored to determine the need to initiate the operation of ESFs. These parameters should be determined by the accident analyses, and may include fuel temperature, core coolant flow and temperature, coolant level, area radiation, and radioactivity of airborne materials. ESF actuation systems need not be designed to be redundant or diverse, or to be able to survive a single failure and still perform the safety function unless the accident analysis requires these features.

The applicant should describe the ESF actuation system in sufficient detail to describe the functions required of the ESF and the operation of the system. The SAR should include the following information for each required ESF actuation system:

- Provide a description of the design criteria for the ESF actuation system as outlined in Section 7.2.1, including any criteria specific to the reactor design not outlined in the section.

- Provide a description of the design bases information for the ESF actuation system as specified in Section 7.2.2 and any additional facility-specific design bases not specified in the general system requirements.

- System description of each ESF actuation system similar to that specified in Section 7.2.3. The description should include:

  - any additional facility-specific system design

  - features of the individual initiation and actuation systems which provide for them to function in concert to prevent or mitigate the consequences of postulated accidents.

- analysis of the operation and performance of each ESF actuation system similar to that specified in the general system requirements of Section 7.2.4, including analysis of the designs of any facility specific features or aspects, including:

  - a discussion of an analysis of the operation and performance of the individual systems which allow them to function in concert to prevent or mitigate the consequences of postulated accidents

  - the bases of any technical specifications, including surveillance tests and intervals specific to the design and operation of the subsystem

The specific design features of the ESF actuation systems that should be addressed include the following:

Design Basis

The RPS initiates rapid control rod insertion to mitigate the consequences of anticipated operating occurrences or design basis events. The ESF actuation systems initiates and controls safety equipment that removes heat or otherwise assist with maintaining the integrity of the physical barriers to radioactive release, such as cladding, coolant pressure boundary, and containment.

Provide a description of the decision criteria for determining which design basis events should be accommodated by functioning of the engineered safety features to mitigate their consequences.

System performance requirements, including system response times, system accuracies, ranges, and rates of change of sensed variables to be accommodated until conclusion of the protective action, should also be identified in the system designation. The system performance requirements should be consistent with the applicable portions of Chapter 13. The licensee should identify the analytical limit associated with each variable and Provide a description of the margin between analytical limits and setpoints.

Provide a description of the reactor variables associated with each Design Basis Event that are monitored by the RPS/ESF actuation systems, including a description of the range, accuracy, and response times of the instrument sensors.

Simple and direct means should be provided for the manual initiation of each protective action (e.g., reactor trip, containment isolation).

Manual initiation of a protective action should perform all actions performed by automatic initiation, such as starting auxiliary or supporting systems, sending signals to appropriate valve-actuating mechanisms to ensure correct valve position, and providing the credited action-sequencing functions and interlocks.

The control interfaces for manual initiation of protective actions should be located in the control room. They should be easily accessible to the operator so that action can be taken in an expeditious manner at the point in time or under the facility's conditions for which the protective actions of the safety system should be initiated. Information displays associated with manual controls should (i) be readily present during the time that manual actuation is necessary, (ii) be visible from the location of the manual controls, and (iii) provide unambiguous indications that will not confuse the operator.

No single failure within the manual, automatic, or common portions of the RPS/ESF actuation systems should prevent initiation of a protective action by manual or automatic means.

Manual initiation of protective actions should depend on the operation of a minimum amount of equipment.

Manual initiation of a protective action should be designed so that, once initiated, the action will go to completion.

The point at which the manual controls are connected to safety equipment should be downstream of the digital I&C safety system outputs. These connections should not compromise the integrity of interconnecting cables and interfaces between local electrical or electronic cabinets and the facility's electromechanical equipment.

Provide a description of the manual controls including the points in time and the operating conditions during which manual control is allowed, the justification for permitting initiation or control subsequent to initiation solely by manual means, the range of environmental conditions imposed upon the operator during normal, abnormal, and accident circumstances throughout which the manual operations should be performed, and the variables that should be displayed for the operator to use in taking manual action. The description should also include confirmation that the controls will be functional (e.g., power will be available and command equipment is appropriately qualified), accessible within the time constraints of operator responses, and available during operating conditions under which manual actions may be necessary.

To the extent feasible and practical, sense and command feature inputs should be derived from signals that are direct measures of the desired variables as specified in the design basis. For example, a safety system that requires loss of flow protection could directly derive its signal from flow sensors. Another design might use an indirect parameter such as a pressure signal or pump speed; however, any indirect parameter should be a valid representation of the desired direct parameter for all events.

Provide a description of for both direct and indirect parameters, the characteristics (e.g., range, accuracy, resolution, response time, sample rate) of the instruments that produce the safety system inputs. Relate these parameters to show consistency with the analysis provided in Chapter 13 of the SAR. Thus, even a directly measured variable should be reviewed and its response to postulated events compared with the credit taken for the parameter in the events for which it provides protection.

Where it is determined that the spatial dependence of a parameter requires several sensor channels to ensure protection of the facility, the redundancy requirements are determined for the individual case. In certain designs, for example, adequate monitoring of core power requires a minimum number of sensors arranged in a given configuration to provide adequate protection. This aspect of redundancy is dealt with in coordination with the organization responsible for reviewing reactor designs to establish redundancy requirements.

Provide a description of and identify the number and location of those variables monitored to manually or automatically, or both, control each protective action that have a spatial dependence (that is, where the variable varies as a function of position in a particular region). The analysis should demonstrate that the number and location of sensors are adequate.

Interlocks ensure that operator actions cannot defeat an automatic safety function during any operating condition where that safety function may be required. These interlocks include permissives for manually initiated operating bypasses and interlocks to ensure manually initiated operating bypasses are automatically removed when operating conditions would require the trip functions. Interlocks are also provided to ensure that manually initiated maintenance bypasses can only defeat a single train or channel of the ESF actuation systems but not multiple channels or trains that would impair the system’s ability to function and meet the single-failure criteria.

Where operating requirements necessitate automatic or manual block of a protective function, the block is automatically removed whenever the appropriate permissive conditions are not met. Hardware and software used to achieve automatic removal of the block of a protective function are part of the PSMS and, as such, are designed in accordance with the same criteria as the protective function.

Some operating bypasses may be automatically initiated when the operating permissive condition is sensed by the ESF actuation systems input channel(s). An example of an automatically initiated operating bypass for the ESF actuation systems would be automatically bypassing the high-source-range neutron flux trip by the power range neutron flux.

Some operating bypasses may be manually initiated. These operating bypasses can be manually initiated separately within each ESF actuation systems division when the operating permissive condition is sensed by the ESF actuation systems input channel(s). An example of a manually automatically initiated operating bypass for the ESF actuation systems would be manually bypassing the high-source-range neutron flux trip with high-intermediate-range neutron flux.

All operating bypasses, either manually or automatically initiated, should be automatically removed when the facility moves to an operating regime where the protective action would be required if an accident occurred. Status indication should be provided in the control room for all operating bypasses.

Provide a description of all operating bypasses, either manually or automatically initiated. Provide a description of the permissive conditions that prevent the defeat of safety functions.

The ESF actuation system should remain operable throughout the ranges of operating conditions, which include such items as voltage, frequency, radiation, temperature, humidity, pressure, and vibration.

Equipment should meet its functional requirements during normal environmental conditions and anticipated operational occurrences, the requirements should be specified in the design/purchase specifications. A maintenance/surveillance program based on a vendor's recommendations, which may be supplemented with operating experience, should ensure that equipment meets the specified requirements.

For safety-related computer-based I&C systems, the evidence of qualification should be based on actual environmental conditions, and the records should be retained at a facility in an auditable and readily accessible form for review and use as necessary.

Provide a description of how the RPS equipment is designed to meet the functional performance requirements over the normal range of environmental conditions anticipated within the facility. The licensee should identify normal environmental conditions, including those resulting from anticipated operational occurrences, as applicable, for temperature, pressure, radiation, relative humidity, EMI/RFI, power surge environment, and operational cycling, and maximum hypothetical accidents to which the equipment is qualified.

Data communication between safety channels or between safety and non-safety systems should not inhibit the performance of the safety function. Safety functions are typically separated from non-safety functions such that the non-safety functions cannot prevent the safety system from performing its intended functions. In digital systems, software performing both safety and non-safety functions may reside on the same computer and use the same computer resources. However, equipment that is used for both safety and non-safety functions should be classified as part of the safety system. The term "equipment" includes both software and hardware of the digital systems. For this reason, any software providing non-safety functions that resides on a computer providing a safety function should be classified as a part of the safety system.

Provide a description of those auxiliary features that (1) perform a function that is not required for the safety systems to accomplish their safety functions, and (2) are part of the ESF actuation systems by association (that is, not isolated from the ESF actuation systems). This Provide a description of should show that the system is designed to meet those criteria necessary to ensure that these components, equipment, and systems do not degrade the safety performance of the ESF actuation systems below an acceptable level.

Specific timing requirements may affect system architecture because it may not be possible to get sufficient computational performance for a specific function or group of functions from a single processor, or the locations where functions are performed may be widely separated. Timing requirements may also increase complexity, either by fragmenting the system into multiple processors or by code tuning, which makes the software product harder to understand, verify, or maintain. The digital instrumentation loop often includes the sensor, transmitter, analog-to-digital converter, multiplexer, data communication equipment, demultiplexer, computers, memory devices, controls, and displays. Timing analysis should consider the entire loop.

The level of detail in the architectural description should be sufficient that the staff can determine the number of message delays and computational delays interposed between the sensor and the actuator. An allocation of time delays to elements of the system and software architecture should be available. In initial design phases (e.g., at the point of design certification application), an estimated allocation of time delays to elements of the proposed architecture should be available. Subsequent detailed design and implementation should develop refined timing allocations down to unit levels in the software architecture.

A design should be feasible with currently known methods and representative equipment. Design timing feasibility may be demonstrated by allocating a timing budget to components of the system architecture so that the entire system meets its timing requirements. The timing budget should include internal and external communication delays, with adequate margins.

Any non-deterministic delays should be noted and a basis provided that such delays are not part of any safety functions, nor can the delays impede any protective action.

Software architectural timing requirements should be addressed in a software architectural description. Databases, disk drives, printers, or other equipment or architectural elements subject to halting or failure should not be able to impede protective system action.

Provide an analysis of the real time performance of the ESF actuation systems, from sensor to actuation.

Design Criteria

Single Failure

The general design criteria for the facility should address the need for design redundancy for reactor protective and safety features, so that any single failure of any active component will not prevent safe reactor shutdown or result in unsafe conditions as verified by Chapter 13 analyses.

Because non-power reactors are conservatively designed, few, if any, accidents should require redundant or diverse ESF systems. However, consideration should be given to adding redundancy and diversity to ESF systems if the reactor is of a higher power level (2 MW or greater thermal power level), if an ESF system would be susceptible to loss of capability to function because of a single failure, or if the radiological consequences to the public of the accident that the ESF is designed to protect against would be very serious if the ESF were to not function.

I&C systems should be designed so that a single failure will not prevent the safe shutdown of the reactor.

The SAR should describe the operation of the I&C system and present the analysis of how the system design meets the design criteria and design bases. The Provide a description ofion should include accuracy, reliability, adequacy and timeliness of I&C system action, trip setpoint drift, quality of components and, if required by the analyses, redundancy, independence, and how a single failure affects both its ability to perform its safety function and the effect on operation or safe shutdown of the reactor.

The single failure criterion stated above should be applied to the design of the RPS (i.e., RPS and ESF actuation systems) for each research reactor. Attention should be given to the situation where a credible single failure could both initiate a Design Basis Event and cause the loss of the corresponding protective action at the channel or subsystem level. One such situation is where a control system input signal is derived from a protective instrument channel (a neutron-level channel, for example).

Provide a description of the method of performing a single failure analysis to show that the ESF actuation system are designed not to fail or operate in a mode that would prevent the RPS from performing its designed function, or prevent safe reactor shutdown. The effects of each component failure mode on the overall system performance should be discussed. In this process, the component failure modes that could contribute to unsafe system failure are identified, and necessary action can be taken at this point in the procedure. The Provide a description ofion should demonstrates that:

- All credible failures in the ESF actuation systems are detectable (through self-diagnosis or manual surveillance tests).
- No credible single failure in the ESF actuation systems will prevent actuation of the RPS.
- No credible single failure in the ESF actuation systems will result in spurious actuation of the RPS, which results in a reactor trip.
- The RPS will fail to the safe state for all credible failures (e.g., the safe state for the RPS is trip whereas the safe state for the ESF actuation systems may be as-is).

Traditionally, diversity is used to protect against design inadequacies. If digital technology is used in the implementation, diversity should be considered to protect against implementation inadequacies.

Assessments of adequate diversity in safety systems generally consider the following six attributes:

- design diversity,
- equipment diversity,
- functional diversity,
- human diversity,
- signal diversity, and
- software diversity.

As addressed in Section 7.2.1, the I&C systems should be designed to have functional reliability, including redundancy and diversity, commensurate with the safety functions to be performed and the consequences of failure of the system to perform the safety function.

There should be at least two completely independent power level scram channels and they should provide diversity and redundancy. That is, the I&C system should be designed to perform its protective function after experiencing a single random active failure within the system. For example, the GA uses both the computer watchdog scram and the digital NM-1000 scram that provides diversity and redundancy to the scram system.

With the introduction of computers as a part of a safety system, concerns have arisen over the possibility that the use of computer software could result in a common-mode failure. Diversity is one method of addressing this concern.

The two principal factors for defense against common-cause failures (CCFs) are quality and diversity. Maintaining high quality will increase the reliability of both individual components and complete systems. Diversity in assigned functions (for both equipment and human activities), equipment, hardware, and software can reduce the consequences of a common-mode failure. The ESF actuation systems should incorporate 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. The diverse means may actuate the same protective function or different protective functions, and may be automatically or manually activated, consistent with the response time requirements of the function.

Consideration of the SAR analyses for the ESF actuation systems 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.

Demonstrate that vulnerabilities of the ESF actuation systems to CCFs are adequately addressed. Where indicated by the SAR analysis as being necessary, a diverse means should be provided for initiating the affected ESF actuation systems function or an alternate compensating function to mitigate the consequences of the identified maximum hypothetical accident for which action is required.

Independence

The RPS/ESF actuation systems should be separated from the RCS to the extent that failure of any single component or channel within the RCS, or failure or removal from service of any single component or channel which is common to the RCS and RPS/ESF actuation systems leaves intact a system satisfying all reliability, redundancy, and independence requirements of the protection systems. Interconnection of the RPS/ESF actuation systems and the RCS should be limited so as to assure that safety is not significantly impaired.

To satisfy the requirements of independence, the safety system functions should maintain their independence between redundant portions of the safety system and between safety systems and other systems. The aspects of independence are:

- Physical independence.
- Electrical independence.
- Communications independence.

Physical independence can be achieved through physical separation (e.g., separate wireways, cable trays, and penetrations), or barriers (e.g., cabinets or rooms).

Electrical independence includes more than the use of separate power sources. To ensure electrical independence, fiber optic cables or qualified isolators can be used to interface all signals between equipment.

For digital interfaces, communications isolation is provided to ensure functional independence between systems. Communication isolation includes communication buffers, which provide separation between communication processing, functional processing, and functional logic, which ensures prioritization of all safety functions.

Communications independence should include confirmation that the routing of signals related to safety maintains (1) proper channeling through the communication systems, and (2) proper data isolation between redundant channels or alternatively, some form of data communication such that data from one channel cannot adversely affect to operation of another channel. Transmission of signals between independent channels should be through isolation devices.

Where data communication exists between different portions of a safety system, the licensee should confirm that a logical or software malfunction in one portion cannot affect the safety functions of the redundant portion(s). If a digital computer system used in a safety system is connected to a digital computer system used in a non-safety system, the licensee should confirm that a logical or software malfunction of the non-safety system cannot affect the functions of the safety system.

The I&C evaluation is limited to the review of components and electrical wiring inside racks, panels, and control boards for systems important to safety. The evaluation of the physical separation of electrical cables is addressed in the review of Chapter 8 of the SAR.

Provide a description of the physical, electrical, and communications independence of the ESF actuation system both within the ESF actuation system channels and between the ESF actuation system and non-safety-related systems. The description should be sufficient to show that the safety system design precludes the use of components that are common to redundant portions of the safety system, such as common switches for actuation, reset, mode, or test; common sensing lines; or any other features which could compromise the independence of redundant portions of the safety system. Physical independence is attained by physical separation and physical barriers.

Equipment Qualification

Electromagnetic interference (EMI), radio-frequency interference (RFI), and power surges have been identified as environmental conditions that can affect the performance of safety-related I&C equipment.

Fiber optics typically offer resistance to such effects but have other attributes that prevent universal acceptability. For example, if the fiber-optic medium may be subject to radiation, fiber that does not become opaque or brittle under irradiation should be specified, or there should be a defined replacement schedule.

Provide a description of the design, installation, and testing practices for addressing the effects of EMI/RFI and power surges on safety-related ESF actuation systems I&C systems. The information provided should be sufficient to allow a reviewer to confirm that data communication media do not present a fault propagation path for environmental effects, such as high-energy electrical faults or lightning, from one redundant portion of a system to another or from another system to a safety system.

Fail Safe

The accident analyses provide the design bases for any required ESF. The ESF design should be as basic and fail safe as practical. Because non-power reactors are conservatively designed, few, if any, accidents should require redundant or diverse ESF systems. However, consideration should be given to adding redundancy and diversity to ESF systems if the reactor is of a higher power level (2 MW or greater thermal power level), if an ESF system would be susceptible to loss of capability to function because of a single failure, or if the radiological consequences to the public of the accident that the ESF is designed to protect against would be very serious if the ESF were to not function.

All non-power reactors should be designed for reactor shutdown in the event normal electrical power is lost. This includes the fail-safe actuation of the control rods. Some non-power reactors may also require emergency power to maintain the shutdown reactor in a safe condition. Some examples of uses of emergency electrical power follow:

- Power for reactor power level monitors, recorders, and necessary safety-related instruments.

- Power for effluent, process, and area radiation monitors, including recorders.

- Power for physical security control systems, information systems, or communications. (In this section, the applicant should only mention the existence of such emergency electrical power and should confine details to the facility physical security plan.)

- Placing or maintaining experimental equipment in a safe condition.

- Power for active confinement or containment engineered safety feature (ESF) equipment and control systems, such as blowers, fans, or dampers, and heating, ventilation, and air conditioning equipment. (This is the equipment necessary to maintain equipment and personnel habitability or to control concentrations or release of airborne radioactive material and to mitigate accident consequences.)

- Power for coolant pumps or systems that remove residual heat from the fuel.

- Power for the emergency core cooling system, including I&C systems.

- Power for other ESF equipment, if applicable.

- Power for emergency area lighting and communication equipment.

- Power for those instrument and control systems necessary to monitor reactor shutdown. (These could include fuel temperature, control rod positions, or fission product monitors.)

Provide a description of the electrical power needs for the ESF actuation systems I&C system and the safe states or priority logic associated with a loss of power event.

Setpoints

For setpoints that have a significant importance to safety, a rigorous setpoint methodology should be used. The methodologies utilized should be documented and appropriate justification for their use should be provided.

Because all measurements are imperfect attempts to ascertain an exact natural condition, the actual magnitude of the quantity can never be known. Therefore, the actual value of the error in the measurement of a quantity is also unknown. There are a number of recognized methods for combining instrumentation uncertainties such as the statistical square root sum of squares (SRSS) methods to combine random uncertainties and then algebraically combine the nonrandom terms with the result.

Provide a description of the methodology used to determine the setpoints for the ESF actuation systems, including a description of the uncertainties associated with the parameters used.

10 CFR 50.36(c)(1)(ii)(A), “Technical Specifications,” requires that, where a limiting safety system setting (LSSS) is specified for a variable on which a safety limit has been placed, the setting be so chosen that automatic protective action will correct the abnormal situation before a safety level is exceeded. LSSSs are settings for automatic protective devices related to variables with significant safety functions. Setpoints found to exceed technical specification limits are considered as malfunctions of an automatic safety system. Such an occurrence could challenge the integrity of the reactor core, reactor coolant pressure boundary, containment, and associated systems.

Accident analyses establish the limits for critical process parameters. These analytical limits, as established by accident analyses, do not normally include considerations for the accuracy (uncertainty) of installed instrumentation. Additional analyses and procedures are necessary to assure that the limiting trip setpoint of each safety control function is appropriate.

Provide a description of the physical features of the ESF actuation system that assure that the proper setpoints are automatically made active or include features that facilitate administrative controls to verify the proper setpoints, or both, when the operating mode of the reactor is changed.

Operational Bypass/Permissives

Any individual channels for which bypassing is allowed during reactor operation should be justified in the SAR. Only minimal bypassing should be permitted in safety systems and never in a system that could compromise scram capability of the other channels.

The purpose of interlocks is to maintain the ESF actuation system in a state that assures its availability in an accident. For the I&C systems, interlocks are used to isolate safety systems from non-safety systems, and interlocks to preclude inadvertent inter-ties between redundant or diverse safety systems where such inter-ties exist for the purposes of testing or maintenance.

The requirement for automatic removal of operational bypasses means that the reactor operator should have no role in such removal. The operator may take action to prevent the unnecessary initiation of a protective action.

Whenever the applicable permissive conditions are not met, a safety system feature that physically prevents or facilitates administrative controls to prevent unauthorized use of bypasses. If operating conditions change so that an activated operating bypass is no longer permissible, the safety system should automatically accomplish one of the following actions:

- Remove the appropriate active operating bypass(es).
- Restore operating conditions so that permissive conditions once again exist.
- Initiate the appropriate safety function(s).

The requirement for automatic removal of operational bypasses means that the reactor operator should have no role in such removal. The operator may take action to prevent the unnecessary initiation of a protective action.

Provide a description of the interlocks within the ESF actuation system, the conditions for their initiation and removal, and which conditions are manual, automatic, or both.

Completion of Protective Actions

The ESF system should be designed so that once initiated—either automatically or manually—the intended sequence of protective actions of the execute features should continue until completion.

The licensee could use functional and logic diagrams to show that “seal-in” features are provided to enable system-level protective actions to go to completion. The seal-in feature may incorporate a time delay as appropriate for the safety function. Additionally, the seal-in feature need not function until it is confirmed that a valid protective command has been received, provided the system meets response time requirements. . 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.

Provide a description of those features used to ensure that the intended sequences of protective actions continue until completion.

Surveillance

I&C systems undergo testing and calibration to maintain reliable and accurate performance.

Testing should confirm operability of both the automatic and manual circuitry and should duplicate, as closely as practical, the overall performance required of the safety system. When this capability can only be achieved by overlapping tests, the test scheme may be such that the tests do, in fact, overlap from one test segment to another. Test procedures that require disconnecting wires, installing jumpers, or other similar modifications of the installed equipment are not acceptable test procedures for use during power operation.

One benefit of digital I&C systems is the use of self-testing, which is a test or series of tests performed by a device upon itself. Self-tests include on-line continuous self-diagnostics, equipment-initiated self-diagnostics, and operator-initiated self-diagnostics. Self-testing can be used for the early identification of inoperable equipment. When self-diagnostics are applied, the following self-diagnostic features should be incorporated into the system design: Self-diagnostics during computer system startup, periodic self-diagnostics while the computer system is operating, and self-diagnostic test failure reporting.

Other self-testing features that are candidates for incorporation into digital computer-based I&C systems include plausibility checks for intermediate results, evaluation using different methods, ranges of variables, array bound checking, well-defined outputs for detected failures, reporting of errors for which error recovery techniques are used, use of counters and reasonableness traps, and correctness verification of transferred parameters.

Although self-testing can be used to ensure reliable and accurate performance, for digital computer-based systems, test provisions should address the increased potential for subtle system failures such as data errors and computer lockup.

Calibration, especially in analog systems, is used to address instrument drift, inaccuracies, and errors. The performance of analog systems can typically be predicted by the use of engineering models. Digital I&C systems are fundamentally different from analog I&C systems in that minor errors in design and implementation can cause them to exhibit unexpected behavior. Inspection and testing are used to verify correct implementation and to validate desired functionality of the final product, in both analog and digital systems.

Provide a summary of the calibration, inspection, and testing (including self-tests and surveillance tests) to confirm operability of the desired functionality of the ESF actuation systems.

All reactor licensees are required by 10 CFR 50.36(c) to specify safety limits in the technical specifications. These safety limits should be placed on important process variables identified in the SAR as necessary to reasonably protect the integrity of the primary barrier against the uncontrolled release of radioactivity.

Surveillance tests are conducted specifically to confirm compliance with TS surveillance requirements. The SAR should provide the bases of any technical specifications, including surveillance tests and intervals specific to the design and operation of the subsystem. The licensee should describe how the proposed design and the justification for test intervals are consistent with the surveillance testing proposed as part of the facility's TS.

If automatic test features are credited with performing surveillance test functions, provisions should be made to confirm the execution of the automatic tests during plant operation. The capability to periodically test and calibrate the automatic test equipment should also be provided. The balance of surveillance and test functions that are not performed by the automatic test feature should be performed manually

Provide a summary of its TS and the bases for the surveillance intervals used in its safety analyses.

If the ESF actuation system is designed to permit periodic testing of its functioning when the reactor is in operation, the ESF actuation systems' design should retain the capability to accomplish its safety function while under test. Where on-line periodic testing is necessary or provided, such testing should not reduce the capability of the RSS below a level of reliability and redundancy such that the RSS can, as a minimum, perform the required protective actions in the presence of any single failure.

In the event that the disabling of a channel (for example, by the disconnection of a detector) is necessary to conduct a surveillance activity, the RSS should include either features which physically assure that operability is restored before allowing any operation of the reactor for which the operability is required or features which facilitate administrative controls which specifically accomplish the same function; for example, a prestart instrument checklist.

Provide a description of the capabilities of the ESF actuation systems to operate while undergoing testing.

Classification and Identification

In order to provide assurance that the design, construction, maintenance, and operation of the facility meet the design criteria, the licensee should describe the following:

- How safety system equipment should be identified for each redundant portion of a safety system,

- How the identification of safety system equipment is distinguishable from any identifying markings placed on equipment for other purposes (for example, identification of fire protection equipment, phase identification of power cables).

One acceptable method of identification is color coding of components, cables, and cabinets.

Provide a description of how the safety system equipment is identified for each redundant portion of a safety system and how the identification of safety system equipment is distinguishable from any identifying markings placed on equipment for other purposes.

Human Factors

Human factors engineering principles and criteria should be applied to the selection and design of the displays and controls. Human-performance requirements should be described and related to the facility's safety criteria. Recognized human-factors standards and design techniques should be employed to support the described human-performance requirements.

Provide a summary of the human-machine interface principles used in the location of instrumentation and controls for the ESF actuation systems.

Quality

10CFR50.55a(a)(1) requires that structures, systems, and components be designed, fabricated, erected, constructed, tested, and inspected to quality standards commensurate with the importance of the safety function to be performed. The design of the control system should be of sufficient quality to limit the potential for inadvertent actuation and challenges to safety systems. While the design of a control system that minimizes inadvertent actuations and challenges to a safety system is good practice, there is no specific requirement for such design practice in reactor applications for which no transients occur. That is, inadvertent actuation may not be a concern for research reactors below 2 MW and TRIGAs.

The engineering design of ESF actuation systems and the components procured for them should be of high quality to ensure reliable operation. This quality is essential because these systems are designed to mitigate the consequences of postulated accidents. Provide a description of the quality program for the ESF actuation systems.

Provide a description of design criteria for the ESF actuation systems and a statement that the criteria and guidelines for implementing those criteria will be implemented in the design of ESF actuation systems.

Managerial and administrative controls are used to assure safe operation. 10 CFR 50.34(a)(7) requires that applicants for construction permits describe a quality assurance program for the design and construction of the structures, systems, and components of the facility. 10 CFR 50.34(b)(6)(ii) requires a description in the SAR of managerial and administrative controls to be used to ensure safe operation. ANSI/ANS 15.8-1995, endorsed by RG 2.5, provides an acceptable method in developing a quality assurance program for the design, construction, testing, modification, and maintenance of research and test reactors for complying with the program requirements of 10CFR50.34.

Provide a description of the overall quality assurance program requirements. The program should identify the items and activities to which it applies and the extent of program application for each item and activity. The program should provide for the appropriate and necessary indoctrination and training of personnel who perform activities that affect quality, to ensure that suitable proficiency is achieved and maintained.

Use of Digital Systems

Because non-power reactors are conservatively designed, few, if any, accidents should require redundant or diverse ESF systems. However, consideration should be given to adding redundancy and diversity to ESF systems if the reactor is of a higher power level (2 MW or greater thermal power level), if an ESF system would be susceptible to loss of capability to function because of a single failure, or if the radiological consequences to the public of the accident that the ESF is designed to protect against would be very serious if the ESF were to not function.

Design techniques, such as functional diversity or diversity in component design and principles of operation, can be used to prevent the loss of the protection function.

The six types of diversity are:

- Design diversity
- Equipment diversity
- Functional diversity
- Human diversity
- Signal diversity
- Software diversity

Example of diversity in the ESF actuation systems are:

1. Functional diversity - monitoring different reactor variables related to the Design Basis Event.

2. Equipment diversity - monitoring the same reactor variable using equipment with different principles of operation.

3. Simple redundancy - monitoring the same reactor variable using duplicate equipment.

Provide a description of the evaluation for adding redundancy and diversity to the ESF actuation systems. If an ESF system would be susceptible to loss of capability to function because of a single failure, or if the radiological consequences to the public of the accident that the ESF is designed to protect against would be very serious if the ESF were to not function.

Software development plans can be used to provide a high-quality software life cycle process. These plans commit to documentation of life cycle activities that enhance the quality of the design features upon which the safety determination is based.

Digital I&C systems are fundamentally different from analog I&C systems. Digital I&C systems can share code, data transmission, data, and process equipment to a greater degree than analog systems. Minor errors in design and implementation can cause them to exhibit unexpected behavior. Consequently, the performance of digital systems over the entire range of input conditions cannot generally be inferred from testing at a sample of input conditions. Inspections, type testing, and acceptance testing of digital systems and components do not alone accomplish design qualification at high confidence levels. To address this issue, the design qualification for digital systems focuses to a large extent on the applicant/licensee employing a high-quality development process that incorporates disciplined specification and implementation of design requirements. nspection and testing are used to verify correct implementation and to validate desired functionality of the final product, but confidence that isolated, discontinuous point failures will not occur derives from the discipline of the development process.

The development of safety system software should progress according to a formally defined life cycle (e.g., Concepts; Requirements; Design; Implementation; Test; Installation, Checkout, and Acceptance Testing; Operation; Maintenance; Retirement). The software developer should select and document the software life cycle, and specify the products that will be produced by that life cycle. The software developer can be the applicant/licensee, the vendor, a company working on behalf of either, or a commercial software development company.

Although not required, specific output documents that formally document the development process and are helpful in also documenting the successful completion/planning throughout the life cycle processes. The information to be reviewed may be contained in the following documents:

- Software Management Plan (SMP).
- Software Development Plan (SDP).
- Software Quality Assurance Plan (SQAP).
- Software Integration Plan (SIntP).
- Software Installation Plan (SInstP).
- Software Maintenance Plan (SMaintP).
- Software Training Plan (STrngP).
- Software Operations Plan (SOP).
- Software Safety Plan (SSP).
- Software Verification and Validation Plan (SVVP).

- Software Configuration Management Plan (SCMP).
- Software Test Plan (STP).

Provide a description of the software development activities. If the software or system development was delegated to others, the authority, duties, verifying, and any activities that can affect the safety-related functions should be discussed.

Because there is not a widely accepted view on software reliability value, determining a failure probability, and therefore a reliability value, is not possible. There is no industry consensus on a method to quantify software reliability and/or availability. Highly reliable software relies very heavily on the software development process to ensure because testing cannot cover all possible conditions that the software may encounter in actual service.

Quantitative reliability determination, using a combination of analysis, testing, and operating experience, can provide an added level of confidence in the reliable performance of the computer system. When reliability goals are identified, the proof of meeting the goals should include the software. The method for determining reliability may include combinations of analysis, field experience, or testing. Reliability of software might be demonstrated by evaluation of the development process combined with testing under a wide range of input conditions. Software error recording and trending may be used in combination with analysis, field experience, or testing. Compensation for the deficiencies in original development process needs to be thorough and systematic to provide confidence that the software will perform its safety function when needed. The qualification method should not rely heavily on operating history for a system that is intended to protect with extraordinarily high reliability against low-frequency events. The normal operating history of the facility is not particularly likely to generate unusual and rare conditions that were not anticipated and which are the cause of a software malfunction.

Provide a description of the software reliability measures and the means for attaining software reliability goals.

Access Control

Physical and electronic access to digital computer-based control system software and data should be controlled to prevent changes by unauthorized personnel. Control should address access via network connections and via maintenance equipment.

Access control uses design features to provide the means to control physical access to safety system equipment, including access to test points and means for changing setpoints. Typically such access control includes provisions such as alarms and locks on safety system panel doors, or control of access to rooms in which safety system equipment is located. Thus, all safety-related digital components and network cabling should be installed in a location in the facility that physically secures the equipment. Portable computer equipment intended to interface with the safety-related equipment should not be used for other purposes, and should not be taken out of and returned to the protected area without appropriate controls and safeguards.

Controls should address access via network connections, and via maintenance equipment. All remote access should be prohibited. Remote access is defined by the safety system's computer security assessment. Wireless connectivity should not be implemented. All wireless capabilities should be disabled on workstations. All wireless capabilities on M&TE equipment should be disabled prior to connecting to safety-related equipment.

Provide a description of those provisions to prevent unauthorized access to hardware and software, throughout the life cycle, for the RPS.

Cyber Security

Computer-based systems are secure from electronic vulnerabilities if unauthorized and inappropriate access and use of those systems is deterred, detected, and mitigated. The security of computer-based systems is established through (1) designing the security features that will meet licensee's security requirements in the systems, (2) developing the systems that do not contain undocumented codes (e.g., back door coding, logic, and/or time bomb codes) and that are resilient to malicious programs (e.g., viruses, worms, and Trojan horses), and (3) installing and maintaining those systems in accordance with the station administrative procedures and the licensee's security program.

Licensees should provide high assurance that digital computer and communication systems and networks are adequately protected against cyber attacks, up to and including the maximum hypothetical accident, from internal and external threats. Licensees should protect from cyber attacks digital computer and communication systems associated with certain categories of functions and support systems and equipment, which, if compromised, would adversely impact the safety-related and important-to-safety functions, security functions, and emergency preparedness functions (including offsite communications) at the facility.

The licensee should:

1. Establish, implement, and maintain a cyber security program for software that provides a protection system function; and

2. Incorporate the cyber security program as a component of the physical protection program.

The cyber security program should be designed to:

1. Implement security controls to protect the ESF ACTUATION SYSTEMS from cyber attacks;

2. Apply and maintain defense-in-depth protective strategies to ensure the capability to detect, respond to, and recover from cyber attacks;

3. Mitigate the adverse affects of cyber attacks; and

4. Ensure that the functions of the ESF ACTUATION SYSTEMS are not adversely impacted due to cyber attacks.

As part of the cyber security program, the licensee should:

1. Ensure that appropriate facility personnel, including contractors, are aware of cyber security requirements and receive the training necessary to perform their assigned duties and responsibilities.

2. Evaluate and manage cyber risks.

3. Ensure that modifications to safety system software or hardware, are evaluated before implementation to ensure that the cyber security performance objectives are maintained.

The licensee should establish, implement, and maintain a cyber security plan that implements the cyber security program requirements of the ESF actuation systems.

1. The cyber security plan should describe how the requirements of this section will be implemented and should account for the site-specific conditions that affect implementation.

2. The cyber security plan should include measures for incident response and recovery for cyber attacks. The cyber security plan should describe how the licensee will:

   i. Maintain the capability for timely detection and response to cyber attacks;

   ii. Mitigate the consequences of cyber attacks;

   iii. Correct exploited vulnerabilities; and

   iv. Restore affected systems, networks, and/or equipment affected by cyber attacks.

The licensee should develop and maintain written policies and implementing procedures to implement the cyber security plan. Policies, implementing procedures, site-specific analysis, and other supporting technical information used by the licensee need not be submitted for Commission review and approval as part of the cyber security plan but are subject to inspection by NRC staff on a periodic basis.

The licensee should review the cyber security program as a component of the physical security program, including the periodicity requirements.

The licensee should retain all records and supporting technical documentation for at least three (3) years after the record is superseded.

- Conclusions about capability, operability, and suitability of the ESF actuation systems requested in **Section 7.2.5**.

7.6 Control Console and Display Instruments

Control console and display instrument systems and equipment include displays for the reactor operator to view such operating information as current values of operating parameters and the status of systems and equipment. The system also enables the operator to control the reactor.

Information displays that are important to safety include the alarms and trip information from the RPS/ESF actuation systems, and the Accident Monitoring System. Errors in these systems can cause reactor operators to take inappropriate actions that further imperil the reactor. Also, since these display systems obtain information from the RPS/ESF actuation systems communication subsystems, faults in display system communications cannot be allowed to propagate back to reactor protection system communication systems, and faults in the RPS/ESF actuation systems communication software cannot vitiate the value of the display system just when it is needed most. A particular problem is reporting faults in display communication systems themselves—the fault may make it impossible to report itself.

The applicant should describe how the control console and display instruments have been designed to collect and display the operating information in such a manner that it can be readily observed and interpreted by the operator. It should describe how the manual control inputs (pushbuttons, switches, and other equipment) have been grouped, oriented, and located with respect to the relevant display instruments to enable the operator to best observe and interpret the operating information and thereby take prompt and accurate steps to supply control inputs on which the reactor control systems can act. In addition, the combined and integrated functioning of the control console and display system should be described to demonstrate how major equipment is designed to function as an integrated information-handling system to readily aid the operator in controlling operation of the reactor. The control console design should prevent unauthorized operation of the reactor.

The advancement of digital technology has simplified the ability to gather, analyze, manipulate, and display large amounts of data. A number of licensees have considered adding internally developed operator information display systems and operating aids to their I&C systems. If these systems digitally process control console information and present this information to the reactor operator to inform the operator of the status of the reactor, or if the operator uses such information to make decisions about the operation of the reactor, the systems need to go through the same review, including verification and validation of software as a digital RCS or CONTROL CONSOLE, DISPLAY INSTRUMENTS, AND EQUIPMENT. It is acceptable to locate these systems in areas where they cannot be viewed by the reactor operator. The applicant should ensure that any interface between the information display system and the control console is isolated. The SAR system design criteria and basis information should include a system description and a system performance analysis for each instrument system or major equipment connected to or displayed at the control console. The description and analysis should be similar to those specified in Section 7.2 and should address the following:

- the outputs, controls, and operator interfaces
- how the output instruments are placed and how they are related to the reactor and other system controls in the main console and auxiliary control room racks
- drawings or photographs showing the arrangement of the display instruments and console control equipment
- sufficient reactor-specific information for operators to understand functions of both analog and digital systems, including connections and interaction between them, and both redundancy and diversity of such systems

- the conclusion about operability and suitability for human factors as requested in the general system recommendations of Section 7.2.

The term “Highly-Integrated Control Room” (HICR) refers to a control room in which the traditional control panels, with their assorted gauges, indicating lights, control switches, annunciators, etc., are replaced by computer-driven consolidated operator interfaces. In an HICR:

- The primary means for providing information to the operator is by way of computer-driven display screens mounted on consoles or on the control room walls.
- The primary means for the operator to command the facility is by way of touch screens, keyboards, pointing devices or other computer-based provisions.

A digital workstation is in essence just one device. Unlike a conventional control panel, there is no way for its many functions to be independent of or separated from one another, because they all use the same display screen, processing equipment, operator interface devices, etc. Functions that should be independent should be implemented in independent workstations. Controls and indications from all safety divisions can be combined into a single integrated workstation while maintaining separation, isolation, and independence among redundant channels.

Typically, data-handling systems such as the post-accident monitoring system, display system, plant computer, or operator console that display and store data from the RPS or ESF actuation system are not safety grade. The RCS may use either sensor data or an output from the safety system. The concern of safety-to-non safety communications is isolation to protect the propagation of a fault from a non safety system to a safety system.

The applicant should include the following for each Control Console and Display Systems:

- Discuss the design criteria for the RCS as outlined in **Section 7.2.1**, including any criteria specific to the reactor design not outlined in the section.

- Discuss the design bases information specified in **Section 7.2.2** and any additional design bases of facility-specific subsystems.

- Describe the system as specified in **Section 7.2.3**, including any additional system descriptive material specific to subsystem design and implementation not covered in Section 7.2.

- Analyze the operation and performance of the system as specified in **Section 7.2.4** including analyses and results of any features or aspects specific to the facility design and implementation not specified in Section 7.2. Include the bases of any technical specifications and surveillance tests with intervals specific to the design and operation of the systems. Address the specific design features of the RCS, such as the following:

Design Basis

1

The designed range of operation of each control console and display device should be sufficient for the expected range of variation of monitored variables for each mode of operation in which the variable is required for monitoring or controlling the facility. The information should include the analysis of the adequacy of the design to perform the necessary control and actuation of the reactor trip system and ESF actuation system as well as information management, storage, and display functions.

The variables that are monitored in order to provide protective action along with the analytical limit associated with each variable should be provided. The applicable portion provided in Chapter 13 should confirm that the system performance requirements are adequate to ensure completion of protective actions. Performance requirements—including system response times, system accuracies, ranges, and rates of change of sensed variables to be accommodated until conclusion of the protective action—should also be identified in the system designation.

Provide a description of the range of a control console and displays and provide sufficient information to ensure that the range of the instruments cover the accidents identified in the facility's licensing basis documents.

~~Verify that~~ The control room should provide the means to manually initiate, monitor, and control automatically initiated protective actions at the division level.

Simple and direct means should be provided for the manual initiation of each protective action (e.g., reactor trip, containment isolation).

Manual initiation of a protective action should perform all actions performed by automatic initiation, such as starting auxiliary or supporting systems, sending signals to appropriate valve-actuating mechanisms to ensure correct valve position, and providing the credited action-sequencing functions and interlocks.

The control interfaces for manual initiation of protective actions should be located in the control room. They should be easily accessible to the operator so that action can be taken in an expeditious manner at the point in time or under the facility's conditions for which the protective actions of the safety system should be initiated. Information displays associated with manual controls should (i) be readily present during the time that manual actuation is necessary, (ii) be visible from the location of the manual controls, and (iii) provide unambiguous indications that will not confuse the operator.

No single failure within the manual, automatic, or common portions of the RPS/ESF actuation systems should prevent initiation of a protective action by manual or automatic means.

Manual initiation of protective actions should depend on the operation of a minimum amount of equipment.

Manual initiation of a protective action should be designed so that, once initiated, the action will go to completion.

The point at which the manual controls are connected to safety equipment should be downstream of the digital I&C safety system outputs. These connections should not compromise the integrity of interconnecting cables and interfaces between local electrical or electronic cabinets and the facility's electromechanical equipment.

Provide a description of the manual controls including the points in time and the operating conditions during which manual control is allowed, the justification for permitting initiation or control subsequent to initiation solely by manual means, the range of environmental conditions imposed upon the operator during normal, abnormal, and accident circumstances throughout which the manual operations should be performed, and the variables that should be displayed for the operator to use in taking manual action. The description should also include confirmation that the controls will be functional (e.g., power will be available and command equipment is appropriately qualified), accessible within the time constraints of operator responses, and available during operating conditions under which manual actions may be necessary.

Equipment should meet its functional requirements during normal environmental conditions and anticipated operational occurrences, the requirements should be specified in the design/purchase specifications. A maintenance/surveillance program based on a vendor's recommendations, which may be supplemented with operating experience, should ensure that equipment meets the specified requirements.

For safety-related computer-based I&C systems, the evidence of qualification should be based on anticipated environmental conditions, and the records should be retained at a facility in an auditable and readily accessible form for review and use as necessary.

Provide a description of how the control console and display equipment is designed to meet the functional performance requirements over the environmental conditions anticipated within the facility. The licensee should identify normal environmental conditions, including those resulting from anticipated operational occurrences, as applicable, for temperature, pressure, radiation, relative humidity, EMI/RFI, power surge environment, and operational cycling, and maximum hypothetical accidents to which the equipment is required to operate.

Control, safety, and transient rod position indication and limit lights should be displayed on the console and should be readily accessible and understandable to the reactor operator.

Provide a description of control, safety, and rod position indication and limit lights.

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 should be readily accessible and understandable to the reactor operator.

Display instrumentation should provide accurate, complete, and timely information pertinent to safety system status. The information displayed and the characteristics of the displays (e.g., location, range, type, and resolution) should support operator awareness of system and facility status and aid operators to make appropriate decisions. Information displayed on the control console 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. The design should minimize the possibility of ambiguous indications that could be confusing to the operator. The display instrumentation provided for safety system status indication need not be part of the safety systems.

Provide a description of other controls and displays (in addition to control, safety, and rod position indication described above) used to keep parameters with a limiting value and those that can affect the reactivity of the core.

A set of displays and controls (safety or non-safety) should be provided in the control room for manual system-level actuation and control of safety equipment to perform protective actions. Information displays associated with manual controls should:

(i) be readily present during the time that manual actuation is necessary,

(ii) be visible from the location of the manual controls, and

(iii) provide unambiguous indications that will not confuse the operator.

In providing diverse manual initiation of protective actions, a set of independent and diverse displays and manual controls should be provided in the main control room. These displays and controls may be safety or nonsafety. These displays and controls could be those used for manual operator action. The information displays for manually controlled actions should include confirmation that displays are functional (e.g., a reliable source of power will be available and sensors are appropriately qualified) during facility conditions under which manual actions may be necessary.

Provide a description of the displays and controls used for manual control, including a description of its visibility and clarity of information provided.

A control console instrument system failure or malfunction should not prevent the RPS from performing its safety function and should not prevent safe reactor shutdown. If the control console instrumentation is non-safety, data communication between safety channels or between safety and non-safety systems should not inhibit the performance of the safety function.

Because displays have software for data communication (even those that are not touch screen monitors), any failure should not cause a failure of a safety system or prevent the safety system from working. Loss of power, power surges, power interruption, and any other credible event to any operator workstation or controller should not result in spurious actuation or stoppage of any device or system unless that spurious actuation or stoppage is enveloped in the facility’s safety analyses.

Provide a description of the failure modes of the display and control instrumentation and the effects of those failures.

If the design includes remote shutdown stations, those stations should provide appropriate displays so that the operator can monitor the status of the shutdown. Those same displays should not prevent safe reactor shutdown.

If remote shutdown capability or monitoring is available, provide a description of the selection, use, security locations, and functions of each monitoring device, including but not limited to remote area monitors.

Manual capability may be necessary because all of the protection and control systems are digital-computer-based and therefore vulnerable to common-cause failure. These displays and controls provide facility operators with information and control capabilities that are not subject to common-cause failures due to software errors in the facility's automatic digital I&C safety system because they are independent and diverse from that system. The point at which the manual controls are connected to safety equipment should be downstream of the facilities digital I&C safety system outputs. These connections should not compromise the integrity of interconnecting cables and interfaces between local electrical or electronic cabinets and the facility's electromechanical equipment. To achieve system-level actuation at the lowest possible level in the safety system architecture, the controls may be connected either to discrete hardwired components or to simple (e.g., component function can be completely demonstrated by test), dedicated, and diverse, software-based digital equipment that performs the coordinated actuation logic. These connections should not compromise the integrity of interconnecting cables and interfaces between local electrical or electronic cabinets and the facility's electromechanical equipment.

Provide a description of manual control system and its connection to the digital I&C system.

Functional characteristics of the display and control digital components (e.g., range, accuracy, time response, update frequency, update speed, screen change speed) should be sufficient to provide operators with the information needed to place and maintain a facility in a shutdown condition. Time response should be sufficiently fast to perform safety functions and be consistent with Human System Interface response expectations.

Provide a description of the basis used to demonstrate that the assumed values used for instrumentation inaccuracy, calibration uncertainties and error, and time response is acceptable and reasonable.

Design Criteria

Design Criteria : Independence

In the past, information displays only provided a display function and did not require two-way communications. Because modern display systems may include control functions, incorrect functioning of the information displays could prevent the safety function from being preformed when necessary. (This is the same issue as and similar methods are appropriate; however, the display instrumentation need not be part of the safety system. For separate RPS and RCS systems, if a single display is used to display safety and non-safety information, the signals associated with control of the RCS should not initiate or defeat control of the RPS.)

If the communications path is one-way from the safety system to the displays, or if the displays and controls are qualified as safety related, the safety determination is simplified. Two-way communications with non-safety control systems have the same isolation issues as any other non-safety to safety communications. In addition, however, the reviewer should ensure that inadvertent actions, such as an unintended touch on a touch-sensitive display cannot prevent the safety function. Two distinct direct operator actions should be required by the operator to initiate a response.

Provide a description of data communications within and between safety channels and between safety and non-safety systems and how incoming and outgoing message data are stored and segregated. Provide a description of how the safety channels withstand communications faults and any barriers used to isolate systems and channels.

Fail Safe

When required by the safety analysis, the control console instruments and equipment should be designed to assume a safe state, a state that has been demonstrated to be acceptable on some defined basis such as disconnection of the system, loss of energy (e.g., electric power, instrument air), or postulated adverse environments (e.g., extreme heat or cold, fire pressure, steam, water, and radiation) are experienced. The control console and instruments should have a reliable source of emergency power sufficient to sustain operation of specific devices on loss of electrical power.

Provide a description of the safe state for the control console instruments and displays and the defined bases for those states.

Prioritization of functions

A priority function receives device actuation commands from safety and non-safety sources, and sends the command having highest priority to one or more safety-related actuated devices. The actuated device is a safety-related component such as a motor actuated valve, a pump motor, a solenoid operated valve, etc. The priority module should also be safety-related.

Safety-related commands that direct a component to a safe state should always have the highest priority and should override all other commands. Communication isolation for each priority module should be as described in the guidance for interdivisional communications. Software-based prioritization should meet all requirements (quality requirements, V&V, documentation, etc.) applicable to safety-related software. To minimize the probability of failures because of common software, the priority module design should be fully tested. (This refers to proof-of-design testing, not to individual testing of each module and not to surveillance testing.) Automatic testing within a priority module, whether initiated from within the module or triggered from outside, and including failure of automatic testing features, should not inhibit the safety function of the module in any way. The priority module should ensure that the completion of a protective action is not interrupted by commands, conditions, or failures outside the module's own safety division.

Provide a description of the priority functions within the control console and display stations and the proof-of-design tests to verify that it meets its intent as specified. Provide a description of the selection of a particular command to send to an actuator when multiple and conflicting commands exist.

Design Criteria : Surveillance

The control console, display instruments (including touchscreen displays), and equipment used to detect and announce failures should be designed for easy testability and capable of being accurately calibrated.

For digital computer-based systems, test provisions should address the increased potential for subtle system failures such as data errors, failure to refresh, and computer lockup. This review should be coordinated with the 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.

Calibration, especially in analog systems, is used to address instrument drift, inaccuracies, and errors. The performance of analog systems can typically be predicted by the use of engineering models. Inspection and testing are used to verify correct implementation and to validate desired functionality of the final product, in both analog and digital systems.

One benefit of digital I&C systems is the use of self-testing, which is a test or series of tests performed by a device upon itself. Self-tests include on-line continuous self-diagnostics, equipment-initiated self-diagnostics, and operator-initiated self-diagnostics. Self-testing can be used for the early identification of inoperable equipment. When self-diagnostics are applied, the following self-diagnostic features should be incorporated into the system design: Self-diagnostics during computer system startup, periodic self-diagnostics while the computer system is operating, and self-diagnostic test failure reporting.

Test and calibration functions should not adversely affect the ability of the computer to perform its safety function. V&V, configuration management, and QA should be required for test and calibration functions on separate computers (e.g., test and calibration computer) that provide the sole verification of test and calibration data. V&V, configuration management, and QA should be required when the test and calibration function is inherent to the computer that is part of the safety system.

Surveillance tests are conducted to confirm compliance operability of the system.

Provide a summary of the calibration, inspection, and testing (including self-tests and surveillance tests) to confirm operability of the desired functionality of the control console and display instrumentation.

The bases for technical specifications, including surveillance tests and intervals for control console devices, and any bypass conditions should be discussed in this section of the SAR (i.e., Section 7.6). The test and calibration provisions should support the types of testing required by the technical specifications.

10 CFR 50.36(c)(3), “Technical Specifications,” states that surveillance requirements are 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. Maintaining system performance provides the basis for the technical specifications of non-power reactors (Ch. 14), consistent with the safety analysis with respect to reliability, availability, and capability of the RPS.

Provide a summary of its technical specifications and the bases for the surveillance intervals used in its safety analyses.

Design Criteria : Human Factors

The information displayed and the characteristics of the displays (e.g., location, range, type, and resolution) support operator awareness of system and facility’s status and will allow facility’s operators to make appropriate decisions. For example, the output and display devices showing reactor ~~nuclear~~ status should be readily observable by the operator while positioned at the reactor control and manual protection systems.

Human factors engineering (HFE) principles and criteria should be applied to the selection and design of displays and controls. Attention should be paid to integrated displays and controls and especially those that are reconfigurable according to context such as touch screens.

Recognized human-factors standards and design techniques should be employed to support the described human-performance requirements.

Defensive measures that can be used to ensure that alarm, display, and control functions provided by the redundant workstations meet these HFE principles include segmentation, fault tolerance, signal validation, self-testing, error checking, and supervisory watchdog programs.

Changes to displays should be evaluated, especially if touch-screens are used. For example, touch screens, which are commonly used in digital control rooms, can be designed to be clearly understood and reduce the likelihood of operator misoperation. However, without application of good human factors design criteria, the screens can become virtually unreadable and un-navigable.

Provide a summary of the human-machine interface principles used in the location of instrumentation and controls for the control console and displays and in the display screens.

Design Criteria : Annunciators

The annunciator and alarm panels on the control console should 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 primary purpose of alarms is to alert operators that the facility is in an abnormal status. Alarms are used not only to draw operator's attention but also to identify the source and extent of the abnormal status. The alarms are also designed taking into consideration functional and ergonomic aspects, facilitating appropriate operator response.

The main features of alarms are as follows.

- Adequate display to acknowledge and recognize alarm information
- Application of alarm prioritization to avoid alarm avalanche
- Request function from alarm display to relevant system display and alarm response procedures

These functions help operators to identify and diagnose transients. Typical attributes reviewed are reliability, diversity, independence, redundancy, self-test, and alarms for manually controlled actions. Thus, the computers and data links used to process alarms should be redundant. The data links from the safety cabinets (RPS, ESF Actuation Systems, etc.) should be physically and functionally isolated so as not to inhibit the safety system in case of failure of the alarm processing.

Provide a description of alarms and annunciators and their attributes such as reliability, diversity, independence, redundancy, and self-test capabilities.

The reliability of alarms is typically based on the following design aspects: redundancy (includes audible and visual devices); separation between redundant segments; testability (typically through self-diagnosis); an augmented qualification program, which includes software V&V; and similar environmental, seismic, and EMI/RFI specifications. The assessment of reliability of annunciators should consider the effect of possible hardware and software failures and the design features provided to prevent or limit the effects of these failures. Hardware failure conditions to be considered should include failures of portions of the computer itself and failures of portions of communication systems. Hard failures, transient failures, sustained failures, and partial failures should be considered. Software failure conditions to be considered should include, as appropriate, software common-cause failures, cascading failures, and undetected failures.

Provide a description of the reliability and quality of the annunciators that are used to support normal and emergency operations.

Negligible-risk research reactors need not comply with the single-failure criterion for the automatic detection of each Design Basis Event and the immediate execution of the safely shutdown of the reactor. However, under such a design, the facility should include methods that promptly detect unsafe failures and alert the reactor operator. Under these conditions, the fault detection and alarms should be reliable, should not introduce a credible common failure mode, and administrative controls are used to identify appropriate specific actions to be taken upon detection of a fault.

If the safety analysis in the SAR shows that independence of annunciators is necessary to alert operators of the detection of unsafe failures (e.g., in lieu of meeting the single-failure criterion), provide a discussion on the Independence (isolation between safety systems and other systems) of the annunciators.

Because of design and architectural differences between analog and digital systems, traditional provisions for analog systems may not be adequate for digital computer-based systems. Self-diagnostics are part of any digital system and should be done appropriately. For example, self-testing of the annunciators should not interfere with proper system operation. Thus, if the alarm system integrity is checked by self-diagnosis, this testing should not affect alarms and digital control system portion of alarms that have self-diagnosis functions. Typically, when no failures are present, the self-diagnostics do not interfere with normal operation; when a failure occurs, the self-diagnostics identify the failure by the cut-in (interrupt processing) features or announcing the failure.

Provide a description of the surveillance tests and self-test features of each digital computer-based module associated with the annunciators. Describe how the design and implementation of the alarms maintains conformance with the criteria that no failure in the annunciators and associated instrumentation interferes with performance of any safety functions. The surveillance test provisions should be adequate to fulfill the fundamental intent of each surveillance test.

Alarms that are provided for manually controlled actions for which no automatic control is provided and that are required for the safety systems to accomplish their safety functions should be reviewed quality and reliability. The reliability of alarms credited for manual action in the safety analysis should consider the following additional design aspects: prompts for credited manual operator and that those alarms developed through an augmented quality program, which includes software V&V; and diversity of alarms to address CCFs. For example, technical specifications may require a shutdown because of a high temperature in the pool. If the reactor does not scram on high pool temperature, an operator must take action.

Provide a description of those actions for which no automatic controls are provided but manual control is required. The description should include a description of the reliability and quality of the alarms.

Quality

10CFR50.55a(a)(1) requires that structures, systems, and components be designed, fabricated, erected, constructed, tested, and inspected to quality standards commensurate with the importance of the safety function to be performed.

The quality standards and design control measures for the control console, display instruments, and equipment should be provided for verifying or checking the adequacy of design. 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.

Provide a description of design criteria for the control console, display instruments, and equipment and a statement that the criteria and guidelines for implementing those criteria will be implemented in the design of control console and display systems.

Use of Digital Systems

The software for the displays should be developed under a software management program commensurate with the risk associated with its failure or malfunction.

Configuration management (CM) is a significant part of high quality engineering activities. The quality assurance criteria for software is implemented through a configuration management program, which includes criteria for administrative control, design documentation, design interface control, design change control, document control, identification and control of parts and components, and control and retrieval of qualification information associated with parts and components.

While the principles and intentions of traditional configuration management apply equally to software, with software there is a greater emphasis on the design process; the deliverable product is more like a design output. With engineered software, a large amount of the design process information and many intermediate design outputs are associated with the final design output. Relatively many software engineering changes are expected and encountered. Consequently, although similar in intent to hardware configuration management, software configuration management requires a change in emphasis, with expansion of the importance of intermediate design baselines and associated design process information. The needs for robust change management and identification and control of product versions are also substantially increased.

Software changes should be traced to their point of origin, and the software processes affected by the change should be repeated from the point of change to the point of discovery. Proposed changes should be reviewed for their impact on system safety. Status accounting should take place for each set of life cycle activities prior to the completion of those activities. The status accounting should document configuration item identifications, baselines, problem report status, change history and release status.

Provide a description of the following set of activities associated with configuration management of its safety system software:

a. Identification and control of all software designs and code,

b. Identification and control of all software design functional data (e.g., data templates and data bases),

c. Identification and control of all software design interfaces,

d. Control of all software design changes,

e. Control of software documentation (user, operating, and maintenance documentation),

f. Control of software vendor development activities for the supplied safety system software,

g. Control and retrieval of qualification information associated with software designs and code,

h. Software configuration audits, and

i. Status accounting.

The digital computer system equipment for the displays and processor, including hardware, software, firmware, and interfaces, should reviewed to provide assurance that the required computer system hardware and software are installed in the appropriate system configuration.

To provide assurance that the required computer system hardware and software are installed in the appropriate system configuration, the following identification requirements specific to software systems should be met:

i. Firmware and software identification should be used to assure the correct software is installed in the correct hardware component.

ii. Means should be included in the software such that the identification may be retrieved from the firmware using software maintenance tools.

iii. Color coding of components, cables, and cabinets can be used to provide physical identification of the digital computer system hardware.

iv. The identification should be clear and unambiguous. The identification should include the revision level, and should be traceable to configuration control documentation which identifies the changes made by that revision.

Provide a description of any program used to ensure that the correct version of the software/firmware is installed in the correct hardware components.

Evidence that the digital computer system equipment for the displays, including hardware, software, firmware, and interfaces, can perform its required functions should be provided.

Software testing consists of testing the smallest testable units, and then integrating those units into larger testable units, and testing as an integrated unit. This process is repeated until finally the system is tested after installation.

Testing should be performed with the computer functioning with the software and diagnostics that is representative of those used in actual operation. All portions of the computer necessary to accomplish safety functions, or those portions whose operation or failure could impair safety functions, should be exercised during testing. This includes, as appropriate, exercising and monitoring the memory, the central processing unit, inputs, outputs, display functions, diagnostics, associated components, communication paths, and interfaces. Testing should demonstrate that the performance criteria related to safety functions have been met.

In those cases in which traditional qualification processes cannot be applied, an alternative approach to verify that a component is acceptable for use in a safety-related application is commercial grade dedication. The objective of commercial grade dedication is to verify that the item being dedicated is equivalent in quality to equipment developed under the licensees QA program. The dedication process for the computer should entail identification of the physical, performance, and development process requirements necessary to provide adequate confidence that the proposed digital system or component can achieve the safety function. The dedication process should apply to the computer hardware, software, and firmware that are required to accomplish the safety function. The dedication process for software and firmware should include an evaluation of the design process.

Provide a description of the following set of activities for the safety system software:

- test planning, which consists of a test plan that addresses key aspects of the test program, such as scope, risks, tasks, resources, responsibilities, and acceptance (pass or fail) criteria for the software item being tested.

- test specification, which consists of test designs, test cases, and test procedures that contain the detailed procedures and instructions for testing as well as the feature or test case acceptance criteria to be employed during the testing effort should be provided, and

- test reporting, which consists of transmittal reports, test incident reports, test logs, and test summary reports that provide for the recording and summarization of test events and that serve as the basis for evaluating test results. All information in this category is summarized in the test summary report.

The reliability of the digital computer system equipment for the displays, including hardware, software, firmware, and interfaces, should be assessed based on a combination of analysis, field experience, testing, or software error recording and trending.

Because there is not a widely accepted view on software reliability value, determining a failure probability, and therefore a reliability value, is not possible. There is no industry consensus on a method to quantify software reliability and/or availability. Highly reliable software relies very heavily on the software development process to ensure reliable software because testing cannot cover all possible conditions that the software may encounter in actual service.

Quantitative reliability determination, using a combination of analysis, testing, and operating experience, can provide an added level of confidence in the reliable performance of the computer system. When reliability goals are identified, the proof of meeting the goals should include the software. The method for determining reliability may include combinations of analysis, field experience, or testing. Reliability of software might be demonstrated by evaluation of the development process combined with testing under a wide range of input conditions. Software error recording and trending may be used in combination with analysis, field experience, or testing. Compensation for the deficiencies in original development process needs to be thorough and systematic to provide confidence that the software will perform its safety function when needed. The qualification method should not rely heavily on operating history for a system that is intended to protect with extraordinarily high reliability against low-frequency events. The normal facility's operating history is not particularly likely to generate unusual and rare conditions that were not anticipated and which are the cause of a software malfunction.

Provide a description of the software reliability measures and the means for attaining software reliability goals.

Access Control

Reactor operation should be prevented and not authorized without use of a key or combination authentication input at the control console to prevent the unauthorized use of the reactor control.

Physical and electronic access to digital computer-based control system software and data should be controlled to prevent changes by unauthorized personnel. Control should address access via network connections and via maintenance equipment.

Access control uses design features to provide the means to control physical access to safety system equipment, including access to test points and means for changing setpoints. Typically such access control includes provisions such as alarms and locks on safety system panel doors, or control of access to rooms in which safety system equipment is located. Thus, all safety-related digital components and network cabling should be installed in a facility's location that physically secures the equipment. Portable computer equipment intended to interface with the safety-related equipment should not be used for other purposes, and should not be taken out of and returned to the protected area without appropriate controls and safeguards.

Controls used to prevent unauthorized access should address access via network connections, and via maintenance equipment. All remote access should be prohibited. Remote access is defined by the safety system's computer security assessment. Wireless connectivity should not be implemented. All wireless capabilities should be disabled on workstations. All wireless capabilities on maintenance and test equipment should be disabled prior to connecting to safety-related equipment.

Provide a description of those provisions to prevent unauthorized access to hardware and software, throughout the life cycle, for the control console, display instruments, and equipment.

Cyber Security

Computer-based systems are secure from electronic vulnerabilities if unauthorized and inappropriate access and use of those systems is deterred, detected, and mitigated. For control console and display instruments, vulnerabilities can occur because the COTS monitors allow external devices (e.g., flash sticks) can be inserted into the monitor or the monitor software can be changed via external devices. The security of computer-based systems is established through (1) designing the security features that will meet licensee's security requirements in the systems, (2) developing the systems that do not contain undocumented codes (e.g., back door coding, logic, and/or time bomb codes) and that are resilient to malicious programs (e.g., viruses, worms, and Trojan horses), and (3) installing and maintaining those systems in accordance with the station administrative procedures and the licensee's security program.

Licensees should provide high assurance that digital computer and communication systems and networks are adequately protected against cyber attacks, up to and including the maximum hypothetical accident, from internal and external threats. Licensees should protect from cyber attacks digital computer and communication systems associated with certain categories of functions and support systems and equipment, which, if compromised, would adversely impact the safety-related and important-to-safety functions, security functions, and emergency preparedness functions (including offsite communications) at the facility.

- The applicant should discuss the conclusions about capability and suitability of the RCS requested in **Section 7.2.5**.

7.7 Radiation Monitoring Systems

Radiation monitoring instrument systems should be designed to perform several important diverse functions in the operation of a non-power reactor. These monitors should indicate radiation intensity and may be used for reactor operations such as to indicate the following: low coolant level, the need to actuate containment or confinement systems, and the need for personnel radiation protective actions, and to monitor release of radioactive material to the environment. These systems include area radiation monitors, with displays near the instrument location and in the control room. These systems may monitor radioactive effluents in the form of gases, liquids, and airborne particulates and provide continuous air monitoring (CAM) for airborne radioactivity in occupied spaces such as the reactor room. Portable radiation monitors and personal dosimetry systems should also be included to help assess exposure and prevent overexposure of workers and other personnel. The radiation protective instruments and measures should be discussed in detail in Chapter 11, "Radiation Protection Program and Waste Management." The present chapter should concentrate on the I&C aspects of the radiation monitoring systems and should be coordinated with the information in Chapter 11.

The applicant should briefly summarize the radiation-monitoring I&C system for the facility and list the various systems and types of equipment. Since some of the systems may provide input to the RPS or ESF actuation system, radiation monitoring systems should meet the applicable criteria and requirements in Section 7.2 for those systems.

The applicant should include the following for each Radiation Monitoring subsystem:

- Discuss the design criteria for the Radiation Monitoring Systems as outlined in Section 7.2.1, including any criteria specific to the reactor design not outlined in the section.

- Discuss the system design bases information specified in Section 7.2.2 and any additional design bases of facility-specific subsystems.

- Describe the system as specified in Section 7.2.3, including any additional system descriptive material specific to subsystem design and implementation not covered in Section 7.2.

- Analyze the operation and performance of the system as specified in Section 7.2.4 including analyses and results of any features or aspects specific to the facility design and implementation not specified in Section 7.2. Include the bases of any technical specifications and surveillance tests with intervals specific to the design and operation of the systems. Address the specific design features of the radiation monitoring system, such as the following:

  - Radiation monitoring instrument systems should be designed to perform several important diverse functions in the operation of a non-power reactor.

  - These monitors should indicate radiation intensity and may be used for reactor operations such as to indicate the following: low coolant level, the need to actuate containment or confinement systems, and the need for personnel radiation protective actions, and to monitor release of radioactive material to the environment.

  - These systems include area radiation monitors, with displays near the instrument location and in the control room. These systems may monitor radioactive effluents in the form of gases, liquids, and airborne particulates and provide continuous air monitoring (CAM) for airborne radioactivity in occupied spaces such as the reactor room.

  - Portable radiation monitors and personal dosimetry systems should also be included to help assess exposure and prevent overexposure of workers and other personnel.

Specific design features of the Radiation Monitoring Systems that should be addressed include the following:

Design Basis

It is important that operators be informed if the barriers to the release of radioactive materials are being challenged. Performance requirements include system response times, system accuracies, ranges, and rates of change of sensed variables. I t is essential that instrument ranges be selected so that the instrument will always be on scale. Narrow-range instruments may not have the necessary range to track the course of the accident; consequently, multiple instruments with overlapping ranges may be necessary.

The range of radiation monitoring systems should be determined based on worst expected conditions. To cover such a wide detection range, multiple instruments may be required. If two or more instruments are needed to cover a, particular range, overlapping of instrument span should be provided. If the required range of monitoring instrumentation results in a loss of instrumentation sensitivity in the normal operating range, separate instruments should be used.

It is also necessary to be sure that when a range is extended, the sensitivity and accuracy of the instrument are within acceptable limits for monitoring the extended range.

Provide a description of the range of a radiation monitoring channel and provide sufficient information to ensure that the range of the instruments cover the accidents identified in the facility's licensing basis documents.

The applicant should briefly summarize the radiation monitoring I&C system for the facility and list the various systems and types of equipment. Since some of the systems may provide input to the RPS or ESF actuation system, radiation monitoring systems should meet the applicable criteria and requirements in Section 7.2 for those systems.

Equipment that is used for both safety and non-safety functions should be classified as part of the safety system. For this reason, any software providing non-safety functions that resides on a computer providing a safety function should be classified as a part of the safety system. If an applicant/licensee desires that a non-safety function be performed by a safety computer, the software to perform that function should be classified as safety-related, with all the attendant regulatory requirements for safety software, including communications isolation from other non-safety software. If the radiation monitoring systems provide input to the RPS or ESF actuation system, radiation monitoring systems should meet the applicable criteria and requirements in Section 7.2 for those systems.

Provide a description of the radiation monitoring I&C systems for the facility. The description should address both safety and non-safety systems and any communications with the RPS or ESF actuation systems.

Control console and display instrument systems and equipment include displays for the reactor operator to view such operating information as current values of operating parameters and the status of systems and equipment. The system also enables the operator to control the reactor.

These systems include area radiation monitors, with displays near the instrument location and in the control room. These systems may monitor radioactive effluents in the form of gases, liquids, and airborne particulates and provide continuous air monitoring (CAM) for airborne radioactivity in occupied spaces such as the reactor room. Portable radiation monitors and personal dosimetry systems should also be included to help assess exposure and prevent overexposure of workers and other personnel.

Provide a description of the radiation monitors and their purpose. If the monitors are addressed elsewhere in the SAR, these sections should be referenced.

Because of the increasing difficulty in finding spare parts for their original analog I&C systems, many licensees have begun or have plans to upgrade, refurbish, or replace their old analog I&C systems with digital systems. Licensees need to be aware however, of several issues associated with upgrading to a digital system including obsolescence of the digital system (hardware and software) because of the short product life cycle and the associated cost to acquire, store, and maintain a long-term supply of spare parts. Configuration management and cyber security are also vitally important for any upgrade. Further, it should be recognized that the introduction of software and microprocessors could create new failure mechanisms, such as software errors and increased susceptibility to electromagnetic interference. Thus, a conversion from analog to digital I&C systems solves some problems while potentially introducing others. Recognition of the additional risks coupled with good design, engineering, review, and testing can identify and minimize these risks.

Provide a description of the radiation monitoring instrumentation along with an evaluation of any new failure modes introduced by the introduction of digital I&C components.

The instrumentation in the radiation monitoring system should be of high-quality commercial grade and should be selected to withstand the specific service environment.

Equipment should meet its functional requirements during normal environmental conditions and anticipated operational occurrences, the requirements should be specified in the design/purchase specifications. A maintenance/surveillance program based on a vendor's recommendations, which may be supplemented with operating experience, should ensure that equipment meets the specified requirements.

For safety-related computer-based I&C systems, the evidence of qualification should be based on anticipated environmental conditions, and the records should be retained at a facility in an auditable and readily accessible form for review and use as necessary.

Provide a description of the suitability of the radiation monitoring system equipment for its service environment. The description should identify expected environmental conditions, including those resulting from anticipated operational occurrences, as applicable, for temperature, pressure, radiation, relative humidity, EMI/RFI, power surge environment, and operational cycling, and maximum hypothetical accidents to which the equipment is qualified.

The required accuracy of accident monitoring instrument channels should be established based on the assigned function. That is, the accuracy requirements for a radiation monitor whose accuracy is specified in the facility's licensing basis documentation will be much greater than those variables that provide trend or stability information (i.e., it is of primary importance for the operator to know whether the monitored variable is increasing, decreasing, or constant).

To the extent practicable, monitoring instrumentation inputs should be from sensors that directly measure the desired variables. An indirect measurement should be made only when it can be shown by analysis to provide unambiguous information.

Provide a description of the accident monitoring instrumentation and the required accuracy of that instrumentation based on its function.

In general, response times for accident monitoring instruments are not critical. However, they are used in determining whether the I&C systems are designed to successfully accomplish the radiation measurement functions. Typically, the displayed information will lag behind actual conditions because of sensor location, information processing cycle times, and other potential effects on instrument response times. Thus, a one-to-two second delay is acceptable for most monitoring systems. For computer driven displays, the indicated variable will additionally lag real time conditions depending on the update frequency of the display. The update frequency should be fast enough to avoid the potential of misleading the operator with respect to operating conditions.

Provide a description of the response times for the accident monitoring instruments. Digital computer timing should be shown to be consistent with the limiting response times and characteristics of the computer hardware, software, and data communications systems. The means proposed, or used, for verifying a system's timing should be consistent with the design. Testing and/or analytic justification should show that the system meets limiting response times for a reasonable, randomly selected subset of system loads, conditions, and design basis accidents. The subset should include some limiting load conditions and be chosen by persons independent of the persons who designed the system.

Design Criteria

Single Failure

It is standard practice that a non-safety system should not affect the operation of a safety system. Software-based systems should be specifically addressed because they could affect multiple channels.

The radiation monitoring system should be designed not to fail or operate in a mode that would prevent the RPS from performing its safety function, or prevent safe reactor shutdown, or into a state that has been demonstrated to be acceptable on some other defined basis, if conditions such as disconnection of the system, loss of energy, or adverse environments, are experienced. This aspect is typically evaluated through evaluation of a failure modes and effects analysis. The analysis should justify the acceptability of each failure effect.

Computer-based safety systems should, upon detection of inoperable input instruments, automatically place the protective functions associated with the failed instrument(s) into a safe state. Hardware or software failures detected by self-diagnostics should also place a protective function into a safe state or leave the protective function in an existing safe state. Failure of computer system hardware or software should not inhibit manual initiation of protective functions or the operator performance of preplanned emergency or recovery actions.

Provide a description of the analysis used to confirm that the requirements of the single-failure criterion are satisfied.

Radiation monitoring systems, which provide operators with necessary information to verify functioning of RCS, RPS, ESF actuation systems, and operating state, should be impervious to single failures. The I&C systems should be designed to accomplish their radiation measurement functions and provide operators with information necessary for them to determine the status of the facility given a single failure within that system. Single failure includes a single failure of a component or channel, or failure or removal from service of any single component or channel. Meeting the single-failure criterion goes beyond the radiation monitoring system preventing or interfering with functioning of the RPS because radiation monitoring systems directly supply operators with information that affects contingency planning.

Because of the potential for software errors potentially affecting multiple components or channels, the need for diversity to preclude CCFs should be considered.

Provide a review of the independence of the information channels or diverse measurements used to mitigate the effect of a single failure within the radiation monitoring system.

Independence

In separating the safety and non-safety displays, safety DISPLAY processors would manage the displays on the safety DISPLAYs whereas non-safety DISPLAY processors would manage the displays on the non-safety DISPLAYs. A buffering circuit allows two-way communication between the safety computer and the non-safety computer, as long as a buffering circuit is employed in the safety computer. The buffering circuit provides an interface allowing acknowledgment or no acknowledgment of data transfer between channels, collision avoidance, etc. It serves as a buffering feature between the communications link and safety function to assure the integrity of the safety function.

If the safety and nonsafety software reside on the same computer and use the same computer resources, either of the following approaches is acceptable to address the data communication issues:

- Barrier requirements should be identified to provide adequate confidence that the non-safety functions cannot interfere with performance of the safety functions of the software or firmware. The barriers should be designed in accordance with the requirements of the safety system software. The non-safety software is not required to meet these requirements.

- If barriers between the safety software and non-safety software are not implemented, the non-safety software functions should be developed in accordance with the requirements for safety system software.

Provide a description of data communications within and between safety channels and between safety and non-safety systems and how incoming and outgoing message data are stored and segregated. Provide a description of how the safety channels withstand communications faults and any barriers used to isolate systems and channels.

Surveillance

If radiation monitors are tied in to digital system (unlike the current analog systems) and automated testing or self diagnostics are used, periodic verification, including verification of the automated test should be performed.

If continuity of operation is a requirement (and surveillance testing during operation is also a requirement), then the radiation monitoring systems should be designed to permit periodic testing of its functioning when the reactor is in operation, including a capability to test channels independently to determine failures that may have occurred. Where safety system testing during operation of the RTR is required or provided as an option, the RPS design should retain the capability to accomplish its safety function while under test.

To maintain reliable and accurate performance, I&C systems undergo testing and calibration. Calibration, especially in analog systems, is used to address instrument drift, inaccuracies, and errors. The performance of analog systems can typically be predicted by the use of engineering models. Inspection and testing are used to verify correct implementation and to validate desired functionality of the final product, in both analog and digital systems.

One benefit of digital I&C systems is the use of self-testing, which is a test or series of tests performed by a device upon itself. Self-tests include on-line continuous self-diagnostics, equipment-initiated self-diagnostics, and operator-initiated self-diagnostics. Self-testing can be used for the early identification of inoperable equipment. When self-diagnostics are applied, the following self-diagnostic features should be incorporated into the system design: Self-diagnostics during computer system startup, periodic self-diagnostics while the computer system is operating, and self-diagnostic test failure reporting.

Test and calibration functions should not adversely affect the ability of the computer to perform its safety function. V&V, configuration management, and QA should be required for test and calibration functions on separate computers (e.g., test and calibration computer) that provide the sole verification of test and calibration data. V&V, configuration management, and QA should be required when the test and calibration function is inherent to the computer that is part of the safety system.

Surveillance tests are conducted to confirm compliance operability of the system.

Provide a summary of the calibration, inspection, and testing (including self-tests and surveillance tests) to confirm operability of the desired functionality of the radiation monitoring systems.

10 CFR 50.36(c)(3), “Technical Specifications,” states that surveillance requirements are 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. Maintaining system performance provides the basis for the technical specifications of non-power reactors (Ch. 14), consistent with the safety analysis with respect to reliability, availability, and capability of the RPS.

If the instrumentation channel signal is to be used in a computer-based display, recording, or diagnostic program, qualification applies from the sensor up to and including the channel isolation device.

Provide a description of the surveillance tests and test intervals for the radiation monitoring system components. If self-diagnostics are used to increase surveillance intervals, the bases for this should be provided.

Human Factors

The instrumentation should be designed to facilitate the recognition; location, replacement, repair, or adjustment of malfunctioning components or modules.

The radiation monitoring Instrumentation design should minimize the development of conditions that would cause meters, annunciators, recorders, alums, etc., to give anomalous indications potentially confusing to the operator. Human factors analysis should be used in determining type and location of displays.

To the extent practicable, the same instruments should be used for accident monitoring as are used for the normal operations of the facility to enable the operators to use, during accident situations, instruments with which they are most familiar.

Provide a description of the displays for radiation monitoring system variables used for accident monitoring and the use of human factors analyses in the display. The basis for displays and display locations should include functional task analysis results and accepted human factors principles.

Display and Recording

Radiation measurements at a reactor facility may be used for reactor diagnostic or safety purposes. For example, radiation monitoring of reactor coolant or the reactor pool may be used to detect fuel failure. 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 basis for display characteristics for accident monitoring variables should be based on an analysis of the system functions required to respond to an accident and the tasks required of the operator to implement those functions. Display characteristics include variables such as range, instrument accuracy, precision, display format (e.g., status, value, or trend), units, and response time.

Provide a review of the suitability of the display characteristics for the accident monitoring variables.

The following types of variables should be uniquely identified on the control console displays:

- those variables that provide information to indicate whether plant safety functions are being accomplished (e.g., reactivity control, core cooling, maintaining reactor coolant system integrity, and radioactive effluent control) and

- those variables that provide information to indicate the potential for being breached or the actual breach of the barriers to fission product releases (e.g., fuel cladding, coolant pressure boundary, and containment/confinement).

Provide a description of the monitoring system used for diagnostics for safety purposes, including type, number, location, and selection process.

Means should be provided for monitoring the reactor confinement or containment atmosphere, effluent discharge paths, and the facility environs for radioactivity that may be released from postulated accidents.

Provide a description of the monitoring system used for diagnostics for safety purposes, including type, number, location, and selection process.

The accident monitoring variables may be continuously displayed or they may be processed for display on demand. If direct or immediate trend or rate information is essential for operator action, the trend information should be continuously available on dedicated trend displays and selectively available on another redundant trend display (with corresponding recording devices). Intermittent displays such as data loggers and scanning recorders can be used if no significant transient response information is likely to be lost by such devices.

If the radiation monitor can cause a scram its information should be continuously displayed on a console clearly visible to the operators; radiation monitors that do not automatically initiate any actions need not be displayed on a control console. Displays for resolving ambiguity do not have to be of the same variable type as the variables being resolved.

Provide a description and identify those variables continuously displayed or processed for display on demand, their type, and justification based on any operator response required.

Signals from effluent radioactivity monitors and meteorology monitors are recorded for future use. If direct and immediate trend or transient Information is essential for operator Information or action, the recording should be continuously available on redundant dedicated recorders. Otherwise, it may be continuously updated, stored in computer memory, and displayed on demand. Intermittent displays such as date loggers and scanning recorders may be used if no significant transient response information is likely to be lost by such devices.

Provide a description and identify those variables that are and are not recorded for future use, and how and where the data is recorded and stored.

Quality

The instrumentation in the radiation monitoring system should be of high-quality commercial grade and should be selected to withstand the specific service environment.

For construction permits, 10CFR50.55a(a)(1) requires that structures, systems, and components be designed, fabricated, erected, constructed, tested, and inspected to quality standards commensurate with the importance of the safety function to be performed. Licensee's should consider these requirements for operations and maintenance.

The quality standards and design control measures for the radiation monitoring systems should be provided for verifying or checking the adequacy of design. 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.

Provide a description of design criteria for the radiation monitoring systems and a statement that the criteria and guidelines for implementing those criteria will be implemented in the design of those systems.

Use of Digital Systems

In addition to the requirements for hardware, software should incorporate the following activities to improve the quality of the software and its development:

- Software development, including the integration of the computer hardware and software, throughout the lifecycle phases;

- Software tools, including the overall context of the quality control and V&V process, and there should be a method of evaluating the output of the tool;

- Verification and validation, Independent verification and validation requirements, includes those V&V processes that address the computer hardware and software, integration of the digital system components, and the interaction of the resulting computer system with the nuclear power facility. The V&V activities and tasks should include system testing of the final integrated hardware, software, firm-ware, and interfaces.

- Software configuration management, including a determination that any software modifications during the design process and after acceptance of the software for use will be made to the appropriate version and revision of the software. This will involve not only a review of the Software Configuration Management documentation, but also a review of the actual methods being used at both the vendor and licensee sites, to ensure that the methods discussed in the plans are properly implemented.

- Software project risk management, including a review of the documentation showing that the safety analysis activities have been successfully accomplished for each life cycle activity group. In particular, the documentation should show 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.

If the radiation monitoring systems contain specifically developed software, provide a description of the software development activities. If the software or system development was delegated to others, the authority, duties, verifying, and any activities that can affect the safety-related functions should be discussed.

To provide assurance that the required computer system hardware and software are installed in the appropriate system configuration, the following identification requirements specific to software systems should be met:

i. Firmware and software identification should be used to assure the correct software is installed in the correct hardware component.

ii. Means should be included in the software such that the identification may be retrieved from the firmware using software maintenance tools.

iii. Color coding of components, cables, and cabinets can be used to provide physical identification of the digital computer system hardware.

iv. The identification should be clear and unambiguous. The identification should include the revision level, and should be traceable to configuration control documentation which identifies the changes made by that revision.

Provide a description of any program used to ensure that the correct version of the software/firmware is installed in the correct hardware components.

Computer system equipment qualification testing should be performed with the computer functioning with software and diagnostics that are representative of those used in actual operation. All portions of the computer necessary to accomplish safety functions, or those portions whose operation or failure could impair safety functions, should be exercised during testing. This includes, as appropriate, exercising and monitoring the memory, the central processing unit, inputs, outputs, display functions, diagnostics, associated components, communication paths, and interfaces. Testing should demonstrate that the performance criteria related to safety functions have been met.

Acceptance of the qualification process should be based upon evidence that the digital system or component, including hardware, software, firmware, and interfaces, can perform its required functions. The acceptance and its basis should be documented and maintained with the qualification documentation.

In those cases in which traditional qualification processes cannot be applied, an alternative approach to verify that a component is acceptable for use in a safety-related application is commercial grade dedication. The dedication process for the computer should entail identification of the physical, performance, and development process requirements necessary to provide adequate confidence that the proposed digital system or component can achieve the safety function. The dedication process should apply to the computer hardware, software, and firmware that are required to accomplish the safety function. The dedication process for software and firmware should include an evaluation of the design process.

Provide a description of the following set of activities for the safety system software:

- test planning, which consists of a test plan that addresses key aspects of the test program, such as scope, risks, tasks, resources, responsibilities, and acceptance (pass or fail) criteria for the software item being tested.

- test specification, which consists of test designs, test cases, and test procedures that contain the detailed procedures and instructions for testing as well as the feature or test case acceptance criteria to be employed during the testing effort should be provided, and

- test reporting, which consists of transmittal reports, test incident reports, test logs, and test summary reports that provide for the recording and summarization of test events and that serve as the basis for evaluating test results. All information in this category is summarized in the test summary report.

Because determining a failure probability and therefore a reliability value is not possible, the reviewer should access if the software was developed using a high quality process of software design to obtain high quality software. The reliability of digital computers in safety systems can be assessed based on a combination of analysis, field experience, testing, or software error recording and trending.

Quantitative reliability determination, using a combination of analysis, testing, and operating experience, can provide an added level of confidence in the reliable performance of the computer system. When reliability goals are identified, the proof of meeting the goals should include the software. The method for determining reliability may include combinations of analysis, field experience, or testing. Reliability of software might be demonstrated by evaluation of the development process combined with testing under a wide range of input conditions. Software error recording and trending may be used in combination with analysis, field experience, or testing. Compensation for the deficiencies in original development process needs to be thorough and systematic to provide confidence that the software will perform its safety function when needed. The qualification method should not rely heavily on operating history for a system that is intended to protect with extraordinarily high reliability against low-frequency events. The normal facility's operating history is not particularly likely to generate unusual and rare conditions that were not anticipated and which are the cause of a software malfunction.

Provide a description of the software reliability measures and the means for attaining software reliability goals.

Cyber Security

The digital safety system development process should identify and mitigate potential weakness or vulnerabilities in each phase of the digital safety system life cycle that may degrade the Secure Development and Operational Environment (SDOE) or degrade the reliability of the system.

Provide a description of the cyber security program for the radiation monitoring systems.

- The applicant should discuss the conclusions about capability and suitability of the Radiation Monitoring Systems requested in **Section 7.2.5**.

7.8 Bibliography

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.