7.3 Reactor Control System (RED = existing text, BLUE = new text)

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Linear and log neutron flux channels should be used to monitor the core neutron flux while control rods are withdrawn or inserted to increase or decrease reactor -power.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.

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. More specifically, 10CFR50.34(a)(3)(i) requires applicants to provide the principal design criteria for the facility and 10CFR50.34(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 ~~Discuss~~ 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.

  10CFR50.34(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.

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

10CFR50.34(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.

- A ~~Discuss~~ 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.

  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.

- An analysis of ~~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. The applicant should include ~~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 ~~Address~~ the specific design features of the RCS, such as the following:

Design Basis

1 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.

Provide a description of the quality program for the RCS.

2 Managerial and administrative controls are used to assure safe operation. Section 50.34(a)(7) of 10 CFR 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. Section 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.

3-5 The reactor control systems should be capable of maintaining system variables as defined in Section 7.2.3 (including the neutron flux density) within prescribed operating ranges. Thus, the system should monitor variables and systems over their anticipated ranges for normal operation (from subcritical multiplication source level through the full licensed power range) defined in Section 7.2.2, for postulated accidents, and for accident conditions as appropriate 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. The sensors must adequately cover the range of operations and accident conditions and should be based on the accident conditions evaluated in Chapter 13. The sensors in the RCS gives ~~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. ~~through the full licensed power range~~. If multiple detector channels are used, this continuous indication should overlap a minimum of one decade during detector changeover.

6-14 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, the applicant should:

- Provide 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.

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

In addition, the applicant should 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.

A summary of the analysis used to confirm the adequacy of control systems with respect to maintaining variables within operational limits during facility operation and to confirm 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.

15 Show 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.

16 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.

Show 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.

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

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

17 The RCS has a reactor period channel that covers subcritical neutron source multiplication from the approach to critical, through critical, and into the ~~licensed~~ 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, show 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 shall include consideration of reactivity addition accidents (e.g., ramp, pulse, experiments, etc.), as applicable.

18 Demonstrate that any single control system component or channel, or failure or removal from service of any single protection system component or channel which is common to the control and protection systems, shall leave intact a system satisfying all reliability, redundancy, and independence requirements of the protection system.

19 In a reactor designed for pulsing, provide an analysis that shows that the movement of the transient rod ~~should be~~ 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 ~~should indicate~~ 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 ~~should provide~~ interlocks to ensure the position of the rod.

20 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.

21 The control console and display system should indicate the mode of operation. For example, ~~While in "automatic" reactor control mode,~~ 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. ~~being placed in or removed from automatic control.~~

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.

Effects of control system operation/failures

22 The conclusions of the analysis of postulated accidents and accidents as presented in Chapter 13 of the SAR are used to confirm 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 on the protection system. This requirement does not apply to a combined RCS-RPS.

23 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.

The applicant should address failure of any control system component or any auxiliary supporting system for control systems to verify that facility conditions 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 that confirms that the consequential effects of postulated accidents and accidents are bounded by the accident analysis in Chapter 13 of the SAR. Finally, the review should confirm that the safety analysis includes consideration of the effects of both control system action and inaction in assessing the transient response of the facility for accidents and postulated accidents.

24 The system and equipment are designed to assume a safe state on loss of electrical power. The applicant should describe the safe state for a loss of electrical power and those components that must change state for these conditions.

Calibration, Inspection, and Testing

25-26 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 confirm 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.

27 The applicant should plan and describe 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.

Interlocks

28 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.

Describe 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.

29 If applicable to the operation of an experimental facility or an experiment, the applicant should describe conditions in which experiment controls can interact with reactor controls.

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").

Independence

30-31 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 must 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.

Control of Access and Cyber Security

32 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.

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 objectives of access control and cyber security controls 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 must 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 shall meet the requirements for the RPS.

Use of Digital Systems

33 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 confirming 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.

- A description of ~~The applicant should discuss~~ 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.