7.3 Reactor Control System (RED = existing text, BLUE = new text, [#X] = bullet # in NUREG-1537)

Areas of Review

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

- nuclear instruments—including all detector channels designed to monitor or measure nuclear radiations, and possibly fuel temperature within the reactor for operational purposes

- process instruments—instruments designed to measure and display such parameters as coolant flow, temperature, or level; fuel temperature; or air flow parameters within or from the reactor room

- control elements—types, number, function, design, and operating features .:-of reactivity control devices other than fuel elements (coordinate with the review of Chapter 4, "Reactor Description")

- interlocks—circuits or devices to inhibit or prevent an action, such as control rod motion, unless a specified precondition exists. Interlocks are intended to protect personnel or other subsystems from harm.

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

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

- a discussion of the criteria for developing the design bases for the RCS I&C system, including the basis for evaluating the reliability and performance of the I&C systems.

- a review of the criteria for developing the design bases for the RCS I&C system, including the basis for evaluating the reliability and performance of the I&C systems should be provided.

- a review of the design bases of the RCS to confirm that the control systems include the necessary features for manual and automatic control of process variables within prescribed normal operating limits.

- a review to confirm that the RCS is not required for safety and that there is a protection system to protect against failures of the control system.

- a description, including logic, schematics, and functional diagrams, of the overall system and component subsystems. The system description with diagrams and auxiliary information should be sufficiently complete to allow a thorough review of all aspects of the RCS including normal /abnormal operation, maintenance, and accident scenarios.

- analysis of the adequacy of the design to establish conformance to the design bases and criteria for reactor power, rate of power change, and pulsing information

- analysis of the adequacy of the design to establish conformance to the design bases and criteria for information on required process variables to control reactor operation

- application of the functional design and analyses to the development of bases of technical specifications, including surveillance tests and intervals

- RCS failure modes to determine if any malfunction of the RCS could prevent the RPS from performing its safety function, or could prevent safe shutdown of the reactor.

Acceptance Criteria

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

Design Basis

1 The control systems should be designed and of sufficient quality to minimize the potential for challenges to safety systems. Confirm that the licensee has implemented a management control system that references or cites industry standards for the design, purchasing, installing, and testing of the RCS.

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

— ~~For I&C systems that are being upgraded to systems based on digital technology, the applicant should consult NRC Generic Letter 95-02, "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."~~ [NOTE: Because this applies to all sections it was updated and moved to the introduction of Chapter 7.]

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

4 Verify that the ~~The~~ RCS provides ~~should give~~ continuous indication of the neutron flux from subcritical source multiplication level through the licensed maximum

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

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

6 Confirm that the ~~The~~ system provides ~~should give~~ reliable reactor power level and rate-of-change information from detectors or sensors that directly monitor the neutron flux.

7 Confirm that the ~~The~~ system provides ~~should give~~ reliable information about the status and magnitude of process variables necessary for the full range of normal reactor operation.

8 Confirm that the ~~The~~ system is ~~should be~~ designed with sufficient control of reactivity for all required reactor operations including pulsing, and to ensure compliance with analyzed requirements on excess reactivity and shutdown margins.

9 Confirm that the ~~The~~ RCS provides ~~should give~~ redundant reactor power level indication through the licensed power range (i.e., redundant sensors with their own display).

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

11 Confirm that a ~~A~~ startup channel with interlock provides ~~should give~~ indication of neutrons and should prevent reactor startup (increase in reactivity) without sufficient neutrons in the core.

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

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

14 The automatic and manual control element absorber, drive, and display systems are

~~should be~~ designed to limit reactor periods and power oscillations and levels to values found acceptable in the reactor dynamic analyses in Chapter 4 of the SAR, and rod and driver positions should be clearly indicated for operator or interlock use.

15 ~~The RCS should be designed for reliable operation in the normal range of environmental conditions anticipated within the facility.~~ Verify that the licensee has shown that the specifications on the I&C are within the bounds of the normal range of environmental conditions.

16 Technical specifications, including surveillance tests and intervals, should be based on SAR analyses and should give the necessary confidence in availability and reliable operation of detection channels and control elements and devices.

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

17 If required by the SAR analysis, confirm that the system provides ~~should give~~ a reactor period or a startup rate indication that covers subcritical neutron multiplication, the approach to critical, through critical, into the ~~operating~~ power range.

18 Confirm that all interfaces between control systems and protection systems have been properly identified and addressed, thereby preserving the reliability, redundancy, and independence requirements of the protection system.

19 For reactors designed for pulsing or "square-wave" operation, confirm that the transient rod and its driver mechanism, interlocks, mode switching, detector channels, other related instruments, and limiting technical specifications are ~~should be~~ designed for the highest possible reliability to ensure that analyzed fuel safety limits will not be exceeded, and personnel hazards will be controlled. Designs should be compared with such systems accepted by NRC for similar operations or reactors.

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

21 Confirm that the control console and display system indicates the mode of operation, status, and change of status of the reactor control mode at all times for

facilities with any automatic control modes.

Effects of control system operation/failures

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

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

24 Confirm that the RCS is ~~The RCS should be~~ designed to assume a safe state on loss of electrical power (i.e., shutdown).

Calibration, Inspection, and Testing

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

26 Confirm that the description of the control elements, their drivers, and display or interlock components demonstrate that they ~~The applicant should plan and discuss 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.

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

Interlocks

28 Verify that the ~~The~~ applicant ~~should~~ describes in the SAR interlocks to limit personnel hazards or prevent damage to systems during the full range of normal operations and any provisions for testing and bypassing are indicated in the control room. ~~Interlocks on such systems as the following should be described, 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 Verify that experimental facilities or experiments that contain interlocks will not compromise the function of the RCS, or safe reactor shutdown will not be compromised. ~~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 Verify any physical, electrical, and communications independence and isolation between safety system functions and the control system that are relied upon in the accident analysis to ensure execution of safety functions during and subsequent to any potential accident that requires a safety function. Verify that the protection system includes separation and isolation methods to protect the protection system from any malfunctions or failures caused by other systems, including the control system.

31 If independence is assumed in the accident analysis and a digital computer system used in a safety system is connected to a digital computer system used in a non-safety system, verify that credible failures such as a logical or software malfunction of the non-safety system, would not affect the functions of the safety system.

Verify that the SAR considered credible failures of the RCS and the possible need for redundancy to protect the protection system.

Control of Access and Cyber Security

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

Use of Digital Systems

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

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

~~Hardware and software for computerized systems should meet the guidelines of IEEE 7-4.3.2-1993, 'IEEE Standard Criteria for Digital Computers Systems in Safety Systems of Nuclear Power Generating Stations,' and Regulatory Guide (RG) 1.152, "Criteria for Digital Computers in Safety Systems of Nuclear Power Plants," Revision 1, which is attached to Chapter 7 of the format and content guide as Appendix 7.1, and software should meet the guidelines of ANSI/ANS 10.4-1987, Guidelines for the Verification and Validation of Scientific and Engineering Computer Programs for the Nuclear Industry," that apply to non-power reactor systems.~~

~~ANSI/ANS 15.15-1978, 'Criteria for the Reactor Safety Systems of Research Reactors," and ANSI/ANS 15.20 (draft), "Criteria for the Control and Safety Systems for Research Reactors," are general guides for the design,' implementation, and evaluation of I&C systems for non-power reactors and should be used where applicable. A digital control system developed by General Atomics has been reviewed by the stag found acceptable, and installed in several NRC-licensed TRIGA reactors (see Amendment No. 19 to Facility Operating License No. R-84, Docket No. 50-170 for the Armed Forces Radiobiology Research Institute TRIGA reactor, July 23, 1990, and Amendment No. 29 to Facility Operating License No. R-38, Docket No. 5-89 for the General Atomics TRIGA Mark I Reactor, October 4, 1990). A digital control system developed by Atomic Energy Canada Limited has been reviewed by the staff, found acceptable, and installed in an NRC-licensed TRIGA reactor (see Amendment No. 30 to Facility Operating License No. R-2, Docket No. 50-5 for the Penn State Breazeale Reactor, August 6, 1991).~~

Evaluation Findings

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

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

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

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

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

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