

REQUEST FOR ADDITIONAL INFORMATION 227-2020 REVISION 0

2/26/2009

US-APWR Design Certification

Mitsubishi Heavy Industries

Docket No. 52-021

SRP Section: 07.04 - Safe Shutdown Systems

Application Section: Section 07.04 - Safe Shutdown Systems

QUESTIONS for Instrumentation, Controls and Electrical Engineering 1 (AP1000/EPR Projects) (ICE1)

07.04-1

MHI should address the CFR subsections applicable to safe shutdown in Section 7.4 and in Table 7.1-2.

Table 7.1-2 in the Design Control Document (DCD) does not provide a column in its list of systems for safe shutdown systems, 7.4. Because safe shutdown functions are achieved by the PSMS, five columns in Table 7.1-2 of the DCD were checked in this review: RPS, ESFAS, SLS and safety HSI, and the column titled "Related Section in US-APWR DCD." Table 7.1-2 in the DCD cites compliance with all the CFR sections listed in SRP Table 7-1 for systems that provide safe shutdown functions.

07.04-2

MHI is requested to discuss compliance with GDCs 34, 35, and 38 in relation to the safe shutdown systems, any potential common-mode failures, and the propagation of erroneous data. Update Table 7.1-2 if necessary.

Table 7.1-2 in the DCD indicates compliance with the GDC listed in Table 7-1 of the SRP as applicable to Section 7.4, Safe Shutdown Systems, with the exception of GDCs 34, 35 and 38. DCD Table 7.1-2 cites Chapter 5 "Reactor Coolant System and Connected Systems" for conformance to GDC 34, and Chapter 6 "Engineered Safety Features" for conformance to GDCs 35 and 38. The staff conducted a review of the RCS and ESF systems, and concluded that ESF control systems are testable and are operable using either onsite or offsite power (assuming only one source is available). Additionally, controls associated with redundant ESF systems are independent and satisfy the single failure criterion. Therefore, the RHR, emergency core cooling system, and containment heat removal systems satisfy the criteria set forth by GDCs 34, 35 and 38, respectively. Detailed compliance with the GDCs is described in TR MUAP-07004-P(R1). SRP Table 7-1 indicates that GDCs 34, 35, and 38 are required for compliance for safe shutdown systems.

07.04-3

Discuss conformance with RG 1.204 in relation to the safe shutdown systems, and assurance that electrical transients resulting from lightning phenomena do not render

REQUEST FOR ADDITIONAL INFORMATION 227-2020 REVISION 0

safety-related systems inoperable or cause spurious operation of such systems. Update Table 7.1-2 if necessary.

RG 1.204 provides guidance for the design and implementation of lightning protection systems (LPSs) to ensure that electrical transients resulting from lightning phenomena do not render safety-related systems inoperable or cause spurious operation of such systems. Table 7.1-2 in the DCD does not cite conformance with RG 1.204, and references Chapter 8, "Electric Power." The staff conducted a review of the grounding and the LPS in Chapter 8 of the DCD, and concluded that the design of the system is in accordance with the IEEE Std 665, 666, 1050 and C62.23, as endorsed by RG 1.204.

07.04-4

Discuss conformance with RG 1.151 in relation to the safe shutdown systems, and the design and installation of safety-related instrument sensing lines. Update Table 7.1-2 if necessary.

RG 1.151 describes a method acceptable to the staff with regard to the design and installation of safety-related instrument sensing lines in nuclear power plants. Table 7.1-2 in the DCD cites compliance with RG 1.151 only for the RPS yet the column titled "Related Section in US-APWR DCD" cites applicability to DCD Sections 7.2–7.6 (RPS, ESFAS, safe shutdown, information systems important to safety, and interlock systems important to safety, respectively). In the US-APWR, all safety-related instrument sensing lines are connected to the RPS, and the signals are redistributed from this system. Because the RPS satisfies all the criteria set forth by RG 1.151, the criteria are met for the overall system to provide safe shutdown functions. However, the column titled "Related Section in US-APWR DCD" indicates that RG 1.151 is applicable to Section 7.4—the section for safe shutdown systems.

07.04-5

Discuss conformance with BTP 7-13 in relation to the safe shutdown systems. Update Table 7.1-2 if necessary.

Only I&C system column "RPS" cites conformance with the BTP 7-13 in Table 7.1-2 in the DCD. This is acceptable because, as explained above for RG 1.151, all safety-related instrument sensing lines go through the RPS before distributed to other systems. Therefore, if RPS complies with BTP 7-13, the overall system for safe shutdown meets the criteria of the staff position. However, the column titled "Related Section in US-APWR DCD" does not indicate that BTP 7-13 is applicable to safe shutdown systems (Section 7.4); SRP Table 7-1 indicates that BTP 7-13 is applicable to safe shutdown systems.

07.04-6

Discuss any features of the ESF systems that are unique to safe shutdown and not directly related to accident mitigation.

REQUEST FOR ADDITIONAL INFORMATION 227-2020 REVISION 0

The review of DCD Section 7.4 evaluates those I&C systems used to achieve and maintain a safe shutdown condition of the plant as required by 10 CFR 50 Appendix A, GDCs 13 and 19. To the extent that the ESF systems are used to achieve and maintain safe shutdown, the review of these systems in this section is limited to those features that are unique to safe shutdown and not directly related to accident mitigation. The features within the scope of SRP Section 7.4 may involve individual component control for safe shutdown versus system-level actuation for accident mitigation, or system-level controls used to achieve and maintain safe shutdown but not used for accident mitigation.

07.04-7

Discuss the applicability of Mode 4—hot shutdown using safety-related plant equipment and what circumstances would this apply? What are the primary functions and related process systems required to achieve and maintain hot shutdown using only safety-related equipment?

The technical specifications for the US-APWR define the modes as any one inclusive combination of core reactivity condition, power level, average reactor coolant temperature, and reactor vessel head closure bolt tensioning with fuel in the reactor vessel. Shutdown functions consist of normal shutdown operation, and safe shutdown operation (i.e., safe shutdown using only safety-related plant equipment). During safe shutdown, reactivity control systems must maintain a subcritical condition of the core, and residual heat removal systems must operate to maintain adequate cooling of the core. Section 7.4.1.6 and its subsections indicates that the US-APWR can achieve hot standby (Mode 3) and cold shutdown (Mode 5) with either the normal or safe shutdown systems.

07.04-8

Identify and discuss any single detectable failure within the safe shutdown systems concurrent with all identifiable but nondetectable failures that were evaluated in the presence of a design basis event.

Section 5.1 of IEEE Std 603-1991 states that the safety system must perform all safety functions required for a design basis event in the presence of (a) any single detectable failure within the safety systems concurrent with all identifiable but nondetectable failures, (b) all failures caused by the single failure, and (c) all failures and spurious system actions that cause or are caused by the design basis event requiring the safety functions. The single failure could occur prior to, or at any time during, the design basis event for which the safety system is required to function. DCD Section 7.4.2.2 states that “all functions . . . including those used to achieve safe shutdown meet the single failure criterion.” Insufficient information is provided to address DBEs, seismic events, and accident conditions.

REQUEST FOR ADDITIONAL INFORMATION 227-2020 REVISION 0

07.04-9

Discuss the conditions and events analyzed where components and systems are assumed to function if functioning adversely affects safety system performance. In addition, discuss the analyses where after assuming the failures of non-safety-grade, non-qualified equipment and those failures caused by a specific event, a random single failure is arbitrarily assumed. With these failures assumed, the safe shutdown system must be capable of performing the protective functions required to mitigate the consequences of the specific event.

SRP Appendix 7.1-C, Subsection 5.1 addresses components and systems not qualified for seismic events or accident environments; non-safety-grade components and systems are assumed to fail to function if failure adversely affects safety system performance. Nonsafety-related components and systems are assumed to function if functioning adversely affects safety system performance. After assuming the failures of non-safety-grade, non-qualified equipment and those failures caused by a specific event, a random single failure is arbitrarily assumed. With these failures assumed, the safety system must be capable of performing the protective functions required to mitigate the consequences of the specific event. DCD Section 7.4.2.2 states that "all functions . . . including those used to achieve safe shutdown meet the single failure criterion." Insufficient information is provided to address DBEs, seismic events, and accident conditions.

07.04-10

Does the design and use of the systems for safe shutdown preclude the use of components that are common to redundant portions of the systems, 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 systems?

Redundant portions of a safety system provided for a safety function shall be independent of and physically separated from each other to the degree necessary to retain the capability to accomplish the safety function during and following any design basis event requiring that safety function. DCD Subsection 7.4.2.4, Independence, states that

Redundant divisions of the RPS, ESFAS, SLS, and safety grade HSI, including those used to achieve safe shutdown, are independent from each other and from the nonsafety division. This independence is also applicable to redundant divisions of safety-related plant instrumentation and component controls for all safe shutdown functions.

This statement indicates physical, electrical, and communications independence within and between channels but does not provide any evidence to substantiate this claim. For example, does the safety system design preclude the use of components that are common to redundant portions of the safe shutdown 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 systems used to achieve and maintain safe shutdown.

REQUEST FOR ADDITIONAL INFORMATION 227-2020 REVISION 0

07.04-11

Is safety system equipment used to achieve safe shutdown functions qualified by type test, previous operating experience, or analysis, or any combination of these three methods? Discuss how these methods will substantiate will be capable of meeting, on a continuing basis, the performance requirements as specified in the design basis. Confirm that the qualification of Class 1E equipment is in accordance with the requirements of IEEE Std 323-1983 and IEEE Std 627-1980.

DCD Subsection 7.4.2.3, Quality of Components and Modules, states that

All functions of the RPS, ESFAS, SLS, and safety grade HSIS, including those used to achieve safe shutdown, are Class 1E, and meet all appropriate quality requirements. Class 1E plant instrumentation and component controls are provided for all safe shutdown functions.

IEEE Std 603-1991 requires that components and modules shall be of a quality that is consistent with minimum maintenance requirements and low failure rates. Safety system equipment shall be designed, manufactured, inspected, installed, tested, operated, and maintained in accordance with a prescribed quality assurance program (ANS/ASME NQA 1-1989). IEEE Std 603-1991 also requires that safety system equipment be qualified by type test, previous operating experience, or analysis, or any combination of these three methods, to substantiate that it will be capable of meeting, on a continuing basis, the performance requirements as specified in the design basis. It further requires that the qualification of Class 1E equipment shall be in accordance with the requirements of IEEE Std 323-1983 and IEEE Std 627-1980.

07.04-12

Is the separation of Class 1E equipment used for safe shutdown in accordance with the requirements of IEEE Std 384-1981? Discuss the physical independence of the equipment used to achieve safe shutdown.

Physical independence is attained by physical separation and physical barriers. Equipment in other systems that is in physical proximity to safety system equipment, but that is neither an associated circuit nor another Class 1E circuit, shall be physically separated from the safety system equipment to the degree necessary to retain the safety systems' capability to accomplish their safety functions in the event of the failure of non-safety equipment. The separation of Class 1E equipment is typically in accordance with the requirements of IEEE Std 384-1981.

07.04-13

Confirm that the routing of signals related to achieving safe shutdown 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 the operation of another channel.

SRP Appendix 7.1-C addresses the transmission of signals between independent channels being through isolation devices. SRP BTP 7-11 addresses the application and

REQUEST FOR ADDITIONAL INFORMATION 227-2020 REVISION 0

qualification of isolation devices. SRP Appendix 7.0-A and SRP Section 7.9 addresses communications independence.

07.04-14

Table 7.4-1, Component Controls for Shutdown, identifies components used for normal and/or safe shutdown. It is assumed then Safe Shutdown components are safety related and Normal Shutdown components may or may not be. Confirm that a logical or software malfunction of the non-safety system cannot affect the functions of the systems used to achieve a safe shutdown.

Where data communication exists between different portions of the safety system used for safe shutdown, a logical or software malfunction in one portion cannot affect the safety functions of the redundant portion(s). In addition, the SLS, RPS, and ESFAS are digital systems that have a communications link with the non-safety PCMS and DAS. Confirm that a logical or software malfunction of the non-safety system cannot affect the functions of the systems used to achieve a safe shutdown.

07.04-15

Table 7.4-1, Component Controls for Shutdown, identifies components used for normal and/or safe shutdown. It is assumed then Safe Shutdown components are safety related and Normal Shutdown components may or may not be safety related. MHI is requested to address the effects of a single random failure in a nonsafety system that can (1) result in a design basis event, and (2) also prevent proper action of a portion of the safe shutdown system designed to protect against that event, and the ability of the remaining portions of the safe shutdown system being capable of providing the safety function even when degraded by any separate single failure.

The safety system design shall be such that credible failures in and consequential actions by other systems shall not prevent the safety systems from meeting the requirements of IEEE Std 603-1991. That is, to address the effects of a single random failure, IEEE Std 603-1991 requires that where a single random failure in a nonsafety system can (1) result in a design basis event, and (2) also prevent proper action of a portion of the safety system designed to protect against that event, the remaining portions of the safety system shall be capable of providing the safety function even when degraded by any separate single failure. See IEEE Std 379-1988 for the application of this requirement.

07.04-16

Address how the operational availability of each sensor will be tested and verified for the systems required to achieve and maintain safe shutdown.

DCD Subsection 7.4.2.5 states that "All functions of the RPS, ESFAS, SLS, and safety grade HSI, including those used to achieve safe shutdown, are periodically tested, as described in Subsection 7.1.3.14." DCD Subsection 7.1.3.14 however, only addresses testing or calibration from the sensor inputs to the actuated equipment or from the

REQUEST FOR ADDITIONAL INFORMATION 227-2020 REVISION 0

sensor to the analog to digital converter. The means for checking the operational availability of each sensor is not addressed.

SRP Appendix 7.1-C and IEEE Std 603-1991 require that means be provided for checking the operational availability of each sensor required for a safety function. For assuring the operational availability of each sense and command feature required during the post-accident period, one means could be checking the operational availability of sensors by use of the methods described in IEEE 603-1991, or by specifying equipment that is stable and retains its calibration during the post-accident time period

Also, the applicant/licensee should state the method to be used for checking the operational availability of non-indicating sensors. Tables 7.2-8 and 7.3-7 analyze sensor failures for Reactor Trip and ESFAS in the PSMS, its' effect, and method of failure detection. DCD Subsection 7.8.2.5 addresses failed sensors for the DAS.

07.04-17

Address the capability of the RSR being able to accommodate a safety injection initiation during cooldown.

SRP Section 7.4 provides guidance for control in locations removed from the MCR that may be used for manual control and alignment of safe shutdown system equipment needed to achieve and maintain hot and cold shutdown. One item is that the remote shutdown capability should be capable of accommodating expected plant response following a reactor trip, including protective system actions that could occur as a result of plant cooldown. For example, in the cooldown of a PWR, reactor cooling system pressure will eventually drop below the safety-injection initiation setpoint. Because the MCR is not available, it may be impossible to block this trip. Therefore, the remote shutdown capability must be able to accommodate this condition.

07.04-18

Discuss the analog plant instrumentation and conventional component controls that are relied on for safe shutdown functions.

DCD Section 7.4.2.6 states that "All functions of the PCMS, used to achieve normal shutdown, and all functions of the RPS, ESFAS, SLS, and safety grade HSI, including those used to achieve safe shutdown, rely on digital systems, as described in Subsections 7.1.3.8 and 7.1.3.17. Analog plant instrumentation and conventional component controls are relied on for normal and safe shutdown functions."

07.04-19

Address the relationship between DCD Section 7.4.1.6.2 and Table 7.4-1 for LOOP events.

All of the required functions for safe shutdown as shown in DCD Section 7.4.1.6.2 do not have automatic starts based on Table 7.4-1. For example, in a LOOP condition, the

REQUEST FOR ADDITIONAL INFORMATION 227-2020 REVISION 0

CCW and ESW pumps automatically start, as does the IAS instrument air compressor and the emergency power generator. Table 7.4-1, Component Controls for Shutdown, shows that the RHR pumps are used for safe shutdown but does not indicate an automatic start for LOOP conditions. Safety plant components are manually loaded on the non-safety alternate ac power source from the SLS during station blackout (which includes a loss of the Class 1E GTG Power Source).