REQUEST FOR ADDITIONAL INFORMATION 705-5495 REVISION 2

2/28/2011

US-APWR Design Certification

Mitsubishi Heavy Industries

Docket No. 52-021

SRP Section: 07.01 - Instrumentation and Controls - Introduction
Application Section: 07.01

QUESTIONS for Instrumentation, Controls and Electrical Engineering 2 (ESBWR/ABWR Projects) (ICE2)

07.01-27

Request to provide clear scope and definition in DCD Section 7.1 for US-APWR design with respect to the “important to safety” and the “augmented quality program.”

The staff has identified a number of instances in MHI’s documents for US-APWR which discuss the I&C systems that are important to safety or of augmented quality but are nonsafety in classification; however, the staff found that their discussions are not consistent throughout. In order to evaluate the extent of the issue, the staff performed a word search for the US-APWR DCD Chapter 7 and respective technical reports with respect to terms of the “important to safety” and the “augmented quality program.” The *partial* word search results are in Attachment 1. The staff finds that there is no clear definition of the design scope to describe the “important to safety” and the “augmented quality program,” and that the staff judges that ITAAC are needed to verify these systems. As seen in the attachment, there are many inconsistent statements to implement these designs.

The staff request MHI to document in DCD Section 7.1 for US-APWR the definition of “important to safety” and the “augmented quality program,” the basis for that determination, the qualification requirements, and the proposed ITAAC to verify that the as-built systems have met the intended function. The staff also request MHI to ensure that the definitions are consistently applied to all relevant documents including all sections of the DCD as well as the technical reports referenced in DCD.

Attachment 1:
References to “Important to Safety” on US-APWR DCD Chapter 7.
Below are all references or mentions of “important to safety” or “augmented quality” for the US-APWR DCD Chapter 7 and respective Technical Reports.
****
US-APWR Design Control Document, Chapter 7, “INSTRUMENTATION AND CONTROLS”
****
“Important to safety”:

- **Section 7.1.1.1, page 7.1-3, 2nd paragraph:**

A brief summary of all the safety-related systems is presented in this section, while more detailed descriptions are given in Section 7.2 for reactor trip system, Section 7.3 for engineered safety feature systems, Section 7.4 for systems required for safe shutdown, Section 7.5 for information systems **important to safety**, and Section 7.6 for interlock

systems **important to safety**. Detailed descriptions of non safety-related systems are described in Section 7.7 for control systems not required for safety, Section 7.8 for diverse instrumentation and control systems, and Section 7.9 for data communication systems.

· **Section 7.1.1.5, "Information Systems Important to Safety," page 7.1-5**

· **Section 7.1.1.6, "Interlock Systems Important to Safety," page 7.1-6**

Interlocks **important to safety** are those that operate to reduce the probability of occurrence of specific events. Interlocks important to safety also ensure availability of ESFs. These interlock logics are implemented within the SLS, which receives process signals from the RPS.

· **Section 7.3.1.2.3, page 7.3-5, 1st paragraph:**

The SLS provides interlocks, which operate to reduce the probability of specific events occurring or to verify the state of a safety system. These include interlocks to prevent over pressurization of low-pressure systems and interlocks to ensure availability of ESF systems. Interlocks **important to safety** are discussed in Section 7.6.

· **Section 7.5.1, page 7.5-1, 1st paragraph:**

This section describes the I&C systems that provide information to the plant operators for: (1) assessing plant conditions and safety system performance, and making decisions related to plant responses to abnormal events; and (2) preplanned manual operator actions related to accident mitigation. The information systems **important to safety** also provide the necessary information from which appropriate actions can be taken to mitigate the consequences of AOOs.

This section describes the following information systems **important to safety**:

• Post accident monitoring (PAM)
• Bypassed and inoperable status indication (BISI)
• Plant annunciators (alarms)
• Safety parameter displays system (SPDS)

Information **important to safety**, which supports emergency response operations, is available via the emergency response data system (ERDS). Refer to Subsection 7.9.1.7.

The information **important to safety** is available for display at the following facilities:

• MCR
• RSR
• TSC
• EOF

· **Section 7.5.1.6, page 7.5-13, 1st paragraph:**

PAM, BISI, plant alarms, and SPDS information is displayed on non-safety HSI equipment at all operations support facilities, including the MCR, RSR, TSC, and EOF. The information displayed in all locations is identical. Duplication of all information **important to safety** at all operations support locations improves the exchange of information between these facilities and the MCR and assists corporate and plant management in the decision-making process.

· **Table 7.5-3 PAM Variables (Sheet 2 of 3), page 7.5-22:**

Status of Standby Power and Other Energy Sources **Important to Safety**
* Class 1E ac Bus Voltage
* Class 1E dc Bus Voltage

· **Table 7.5-9 Function of Type D PAM Variables, page 7.5-29:**

Status of Standby Power and Other Energy Sources **Important to Safety**
* Class 1E ac Bus Voltage
* Class 1E dc Bus Voltage

· **Section 7.6, page 7.6-1:**

This section describes interlock systems **important to safety**. These interlocks are provided to:
• Prevent accident conditions.
• Ensure availability of safety functions.

· **Section 7.6.1, page 7.6-1, 1st and 2nd paragraph:**

The PSMS provides the interlock systems **important to safety** for the plant, with the exception of electro-mechanical interlocks within the electrical distribution system. Except as noted for specific interlocks described below:
There is no manual bypass capability for interlocks **important to safety**.

· **Section 7.6.2, page 7.6-5, 1st paragraph:**

The interlock systems **important to safety** comply with the following codes and standards:
1. 10 CFR 50.55a(a)(1), “Quality Standards.”
2. 10 CFR 50.55a(h), “Protection and Safety Systems,”
3. 10 CFR Part 50, Appendix A, General Design Criterion (GDC) 1, “Quality Standards and Records.”
4. GDC 2, “Design Bases for Protection Against Natural Phenomena.”
5. GDC 4, “Environmental and Dynamic Effects Design Bases.”
6. GDC 13, “Instrumentation and Control.”
7. GDC 19, “Control Room.”
8. GDC 24, “Separation of Protection and Control Systems.”
9. 10 CFR 50.34(f)(2)(v), “Additional TMI-Related Requirements, Bypass and Inoperable Status Indication”

· **Section 7.6.2.2, page 7.6-6:**

All interlocks **important to safety** are implemented using Class 1E components with a corresponding quality program.

· **Section 7.6.2.5, page 7.6-6:**

All interlocks **important to safety** are implemented in the PSMS, which is a digital system. This includes sensor monitoring and bistable functions, and interlock logic. The final SLS output (i.e., open or close), which interfaces to the controlled plant component, reflects the result of combining all manual, automatic and interlock control signals.

· **Section 7.6.3, page 7.6-6, 1st and 3rd paragraph:**

All the interlocks **important to safety** provide protection for plant mechanical systems or protection to prevent plant accident conditions. All the interlocks are implemented by the PSMS.

“Augmented quality program”:

· **Section 7.1.3.16, page 7.1-15, 3rd paragraph:**

The SSA of the PCMS ensures the PCMS does not take erroneous control actions based on a single instrument channel failure or a single RPS train failure. As such, a single failure will not cause the PCMS to take erroneous control actions that challenge the PSMS, while the PSMS is in a degraded operability state due to a failed instrument channel or failed RPS train. The SSA is designed with an **augmented quality program**, including software V&V.

· **Section 7.4.2.3, page 7.4-8, 2nd paragraph:**

The operational VDUs and interfaces to the SLS, which may also be used to achieve normal and safe shutdown, are developed through an **augmented quality program** that includes software V&V, and seismic and environmental testing to levels consistent with the PSMS.

· **Section 7.5.1.3, page 7.5-9, last paragraph:**

The highly reliable design of the alarm system makes it suitable for prompting operator attention to all abnormal plant conditions, including those requiring manual operator

actions credited in the plant safety analysis. The alarms for credited manual operator actions are developed through an **augmented quality program**, which includes software V&V.

· **Section 7.5.1.4, page 7.5-10, last paragraph:**

The computer that processes SPDS functions and all related HSI components are redundant, to ensure operation is not adversely affected by credible malfunctions. SPDS signals originate in plant instrumentation or within the controllers of the PCMS and PSMS. These signals are interfaced to the PCMS via the redundant unit bus, described in Section 7.9. The data interface to the PSMS is physically and functionally isolated so as not to affect the safety system in the event of SPDS component failure. The SPDS is developed through an **augmented quality program**, which includes software V&V.

· **Section 7.5.1.5, page 7.5-12, 2nd paragraph:**

HSI to support all credited manual operator actions is provided on safety VDUs. Operational VDUs and interfaces to the SLS, which may also be used for credited manual operator actions, are developed through an **augmented quality program**, which includes software V&V, and seismic and environmental testing to levels consistent with the PSMS.

· **Section 7.5.1.5.1, page 7.5-12, 1st & 2nd paragraphs:**

The reliability of all PSMS alarms is ensured based on the following design aspects:

· Redundancy is provided for all alarm HSI components including audible and visual devices to ensure no adverse affects by credible malfunctions.
· Separation between redundant segments is provided so that a failure in one segment does not result in the failure of both redundant segments.
· Testability is provided from self-diagnosis of MELTAC and HSI computers.
· An **augmented qualification program** is provided for alarms for credited related to SPDS.
· Similar environmental, seismic, and EMI/RFI specifications are provided as for the PSMS. Conformance testing differs with respect to the QA level and documentation.

The PCMS provides a highly reliable design for all audible and visual alarms. The reliability of alarms credited for manual action in the safety analysis is further ensured from the following additional design aspects.

· Prompts for credited manual operator actions are provided on PCMS non-safety VDUs and PSMS safety VDUs.
· The PCMS alarms for credited manual operator actions are developed through an **augmented quality program**, which includes software V&V.
· Diverse alarms from DHP address CCF in PSMS and/or PCMS.
· The parameters for credited manual operator actions are indicated on the safety VDU to accommodate degraded HSI conditions (i.e., loss of PCMS VDUs), since restricted, continued operation with complete loss of PCMS VDUs is within the US-APWR HSI design basis. Indications on the safety VDU are spatially dedicated and continuously visible (SDCV) and include alarm color coding. The safety VDUs provide notification of the plant accident condition to the operator in case of malfunction of the PCMS VDUs.

· **Section 7.7.2.6, page 7.7-20, 1st paragraph:**

The PCMS and PSMS utilize the same basic software. In addition, the PCMS application software is developed using a structured process similar to that applied to development of the PSMS application software. This process includes an **augmented quality program**, including software V&V, for the following functions:

• Safety functions controlled by operational VDUs
• SPDS
• Alarms for credited manual operator actions

• SSA

· **Section 7.8.2.7, page 7.8-7, 1st paragraph:**

The DAS is a non-safety system designed with augmented quality, as defined by Generic Letter 85-06 (Reference 7.8-5). The following are the key attributes of the **augmented quality program**:

• Designed specially for nuclear applications using a nuclear quality program that meets the US-APWR QAP descriptions and the guidance in GL 85-06.
• Uses components with a long history of successful operation.
• Uses components that are common in conventional non-digital safety systems.
• Follow a design process that includes independent review by people that were not involved in the original design.

****

Technical Report MUAP-07004-P, Rev 5, Safety I&C System Description and Design Process

****

· **Section 3.1, "Code of Federal Regulations," page 2:**

(4) 10 CFR 50.49 Environmental Qualification of Electric Equipment **Important To Safety** For
Nuclear Power Plants

This Equipment is located in a mild environment. A mild environment is an environment that would at no time be significantly more severe than the environment that would occur during normal plant operation, including anticipated operational occurrences. Therefore this criteria is not applicable. This criteria is applicable to some instrumentation that interfaces to this Equipment. The qualification of this instrumentation is described in the US-APWR DCD Chapter 7.

(5) 10 CFR 50.55a

・ (a)(1) Quality Standards for Systems **Important to Safety**

This Equipment was originally developed under a Japanese nuclear quality program that is equivalent to 10CFR50 Appendix B. Other licensing documents describe this equivalence. An approved 10CFR 50 Appendix B quality program is now in effect for all Equipment.

· **Section 4.2.3, c. "Control of Interlocks Important to Safety," page 37:**

Typical examples of the Interlocks Important to Safety are as follows;

・ Interlocks for Residual Heat Removal Heat Exchanger Inlet Isolation Valve
・ Component Cooling Water isolation for non-safety components
・ Interlocks for Accumulator Isolation Valves

The Safety Logic System controls these Interlocks Important to Safety through the component
level application software in the SLS controllers. Non-safety systems are not required for Interlocks Important to Safety.

· **Section 4.2.5, b. "Important to Safety Indication," page 40**

· **Section 6.5.6, "Seismic Analysis Method," page 92"**

Plant structures, systems, and components **important to safety** are required by GDC 2 to withstand the effects of earthquakes without loss of capability to perform their safety functions. The seismic analysis method for the PSMS is based on Regulatory Guide 1.100, which endorses IEEE 344-1987.

· **Section A.6.3, "Interaction between the Sense and Command features and other Systems," page 119:**

The Signal Selection function in the PCMS is considered important to safety. Therefore it is designed and maintained with appropriate Software QA, V&V and Configuration Management. The design process for **important to safety** functions is as follows.
(1) Software development
Signal Selection function is developed the same as any application software of the PSMS.
(2) Software V&V
Software V&V for PCMS Signal Selection Algorithm software is the same as the V&V for the application software of the PSMS.
Software V&V for the Signal Selection application software is done from the PSMS output to the Signal Selection function output.
(3) Configuration Management
The Configuration Management of the application software for the Signal Selection function is the same as the Configuration Management for the PSMS application software.

- **E1. Interdivisional Communications, Staff Position 3.1.5.6, "Analysis," page 186:**

As stated in Appendix C of this Technical Report, the O-VDU is "Seismically qualified for physical and functional integrity to the same Class 1E standards and qualification levels as the PSMS". In addition, Section 7.5.1.5 of the US-APWR DCD states "Operational VDUs …are developed through an **augmented quality program**, which includes software V&V, and seismic and environmental testing to levels consistent with the PSMS. Environmental testing includes EMI/RFI, loss of power, power surges and power interruption conditions, etc. same as for the PSMS".
****
Technical Report MUAP-07005-NP/P, Rev 6, Safety System Digital Platform MELTAC
****

- **Section 6.5, "Engineering Tool Life Cycle," page 184 (non-proprietary version shown here):**

The Engineering Tool was developed and managed under MELCO's Original QAP. It has demonstrated correct performance for nuclear applications of the MELTAC platform since 1987. Since the Engineering Tool is not credited for any safety related functions (ie. the output of the tool is manually verified), the **[ ]** and **[ ]** have not been applied to the Engineering Tool. The tool will continue to be managed under **[ ]**. This is equivalent to an item managed under an Appendix B QAP as a non-safety component with **augmented quality control**. **[ ]** invokes the quality controls described in Section 6.1, above, and the life cycle management controls described in Section 6.2. However, the following sections are not applicable to the Engineering Tool**.**