UNITED STATES
NUCLEAR REGULATORY COMMISSION
ADVISORY COMMITTEE ON REACTOR SAFEGUARDS
WASHINGTON, DC 20555 - 0001

June 25, 2009

Mr. R. W. Borchardt
Executive Director for Operations
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001

SUBJECT: SAFETY EVALUATION FOR THE MITSUBISHI HEAVY INDUSTRIES TOPICAL REPORT MUAP-07006-P, REVISION 2, "DEFENSE-IN-DEPTH AND DIVERSITY," RELATED TO THE US-APWR DESIGN

Dear Mr. Borchardt:

During the 563rd meeting of the Advisory Committee on Reactor Safeguards, June 3-4, 2009, we reviewed the Safety Evaluation (SE) for the Mitsubishi Heavy Industries (MHI) Topical Report MUAP-07006-P, Revision 2, "Defense-in-Depth and Diversity," for the U.S. Advanced Pressurized Water Reactor (US-APWR). Our Subcommittee on US-APWR also reviewed this matter during a meeting on May 21, 2009. During these meetings, we had the benefit of discussions with the staff and other stakeholders. We also had the benefit of the documents referenced.

RECOMMENDATION

The Safety Evaluation for Revision 2 of the MHI Topical Report MUAP-07006-P should be issued.

BACKGROUND

In 2007, MHI submitted the Topical Report MUAP-07006-P to the NRC staff for review. This Topical Report describes the MHI generic methodology used to address defense-in-depth and diversity in digital instrumentation and control (I&C) systems. MHI requested that the staff review and approve a defense-in-depth and diversity (D3) approach for digital I&C systems for the US-APWR and the current operating nuclear power plants.

In 2008, the staff notified MHI that it would be limiting the review of the Topical Report to the US-APWR design. This was due to the difficulty in addressing the unique aspects of the D3 approach in one Topical Report for all operating plants. Therefore, the staff's approval of MHI's D3 approach is limited to the US-APWR design. In addition, some aspects of the D3 approach could not be fully evaluated without reviewing more of the design-specific information in the associated Design Control Document or other topical and technical reports. The staff identified 11 design certification application specific action items to be evaluated during design certification reviews.

DISCUSSION

The MHI digital I&C system is built on the Mitsubishi Electric Total Advanced Controller Platform used in several of the Japanese nuclear power plants. It is a fully digital four channel system that includes a safety-related protection and safety monitoring system (PSMS) and a non-safety plant control and monitoring system (PCMS). The engineered safety features actuation system (ESFAS) is a subsystem of the PSMS. The PSMS includes many design features to minimize the potential for hardware or software failures. However, the design does not rely on these features to meet the regulatory requirements for defense-in-depth and diversity in the event of software common-cause failures (CCF) within the PSMS. To address the potential software CCF events, MHI credits a diverse actuation system (DAS) which is separate from the PSMS and PCMS and is not safety related.

DAS is an analog system with no software-based components. It consists of two trains located in separate fire zones**.** The control panel for DAS is located in the control room. The DAS shares sensor inputs with the PSMS through interfaces that are not subject to postulated software CCFs. The sensors and their isolation devices are analog components. Some of the outputs from the PSMS, PCMS, and DAS use common power interface modules to control or actuate some components. The DAS provides an analog signal to a power interface module that also has a digital input from ESFAS. The power interface module then sends a control signal to the ESFAS components. The staff identified two design certification application specific action items needed to provide assurance that a software CCF within the power interface modules cannot disable both the DAS and ESFAS systems. One application specific action item requires demonstration that the isolation devices are non-software based devices and completely testable. The other application specific action item requires demonstration that the power interface module is not susceptible to a software CCF.

To minimize spurious actuations, both trains of DAS must operate to initiate a reactor scram. DAS is automatically bypassed if it receives feedback from the safety components that they have been actuated by the PSMS. If DAS actuation is necessary, it initiates a reactor scram using means diverse from the PSMS. This is accomplished by shutting off the motor-generator sets that power the rod control system. The staff found that the DAS provides adequate diversity from the PSMS and satisfies the requirements for mitigation of an Anticipated Transient Without Scram (ATWS).

The DAS is automated for Anticipated Operational Occurrences (AOOs) and postulated accidents that require action within 10 minutes. These automatic actions include reactor trip, turbine trip, emergency feedwater actuation, and main feedwater isolation. MHI is proposing to take credit for manual operator actions within the first 30 minutes for certain events. The staff identified this as a design certification application specific action item, to be addressed during the design certification review. The staff will use the guidance from a forthcoming Interim Staff Guidance (ISG), “Crediting Manual Operator Actions for Diverse Actuation of Safety System,” in making its safety determination. The human factors engineering analysis of the time to complete the required manual actions and the adequacy of the plant transient analysis used to establish the time available will be evaluated during the design certification review to assess the acceptability of crediting manual operator actions during the first 30 minutes of a transient.

The coping strategy for large-break loss-of-coolant accidents (LBLOCA) in the Topical Report is based on arguments made by the designers and defensive measures within the design of the RPS/ESFAS, which reduce the potential for CCF concurrent with LBLOCA. These include the quality and reliability of the Mitsubishi Electric Total Advanced Controller design, recognition that CCFs are not triggered by AOOs or postulated accidents, the low frequency of LBLOCAs, and the DAS leak monitoring system. The staff found this coping strategy to be unacceptable because LBLOCAs are possible and leak-before break is not applicable. Therefore, the staff initiated an application specific action item requiring MHI to enhance its coping strategy for the US-APWR and submit it as part of the design certification review.

The staff concluded that the defense-in-depth and diversity approach documented in the Topical Report and responses to the Requests for Additional Information conform with regulatory requirements. This conclusion is subject to the satisfactory completion of the 11 design certification application specific action items documented in the SE. We concur with the staff's conclusion.

The SE for the MHI Topical Report MUAP-07006-P, Revision 2, should be issued.

Sincerely,

/RA/

Mario V. Bonaca
Chairman

References:

- U.S. Nuclear Regulatory Commission, Safety Evaluation by the Office of New Reactors, Licensing Topical Report MUAP-07006-P, Rev. 2, "Defense-in-Depth, and Diversity," dated June 2009 (ML091100381)

- Mitsubishi Heavy Industries, US-APWR Topical Report MUAP-07006-P, Revision 2, "Defense-in-Depth, and Diversity," dated June 2008 (ML081770168)

The coping strategy for large-break loss-of-coolant accidents (LBLOCA) in the Topical Report is based on arguments made by the designers and defensive measures within the design of the RPS/ESFAS, which reduce the potential for CCF concurrent with LBLOCA. These include the quality and reliability of the Mitsubishi Electric Total Advanced Controller design, recognition that CCFs are not triggered by AOOs or postulated accidents, the low frequency of LBLOCAs, and the DAS leak monitoring system. The staff found this coping strategy to be unacceptable because LBLOCAs are possible and leak-before break is not applicable. Therefore, the staff initiated an application specific action item requiring MHI to enhance its coping strategy for the US-APWR and submit it as part of the design certification review.

The staff concluded that the defense-in-depth and diversity approach documented in the Topical Report and responses to the Requests for Additional Information conform with regulatory requirements. This conclusion is subject to the satisfactory completion of the 11 design certification application specific action items documented in the SE. We concur with the staff's conclusion.

The SE for the MHI Topical Report MUAP-07006-P, Revision 2, should be issued.

Sincerely,

/RA/

Mario V. Bonaca
Chairman

References:

- U.S. Nuclear Regulatory Commission, Safety Evaluation by the Office of New Reactors, Licensing Topical Report MUAP-07006-P, Rev. 2, "Defense-in-Depth, and Diversity," dated June 2009 (ML091100381)

- Mitsubishi Heavy Industries, US-APWR Topical Report MUAP-07006-P, Revision 2, "Defense-in-Depth, and Diversity," dated June 2008 (ML081770168)

ACRS Branch A
ACRS Branch B
E. Hackett
H. Nourbakhsh
J. Flack
J. Riner
C. Jaegers
T. Bloomer
B. Champ
A. Bates
S. McKelvin
L. Mike
J. Ridgely
RidsSECYMailCenter
RidsEDOMailCenter
RidsNMSSOD
RidsNSIROD
RidsFSMEOD
RidsRESOD
RidsOIGMailCenter
RidsOGCMailCenter
RidsOCAAMailCenter
RidsOCAMailCenter
RidsNRROD
RidsNROOD
RidsOPAMail
RidsRGN1MailCenter
RidsRGN2MailCenter
RidsRGN3MailCenter
RidsRGN4MailCenter

Accession No: ML091560375 **Publicly Available (Y/N):** Y **Sensitive (Y/N):** N
If Sensitive, which category?
Viewing Rights: ☒ NRC Users or ☐ ACRS only or ☐ See restricted distribution

OFFICE	ACRS	SUNSI Review	ACRS	ACRS	ACRS
NAME	NColeman	NColeman	ADias/CSantos	EHackett	EHackett for MBonaca
DATE	6/25/09	6/25/09	6/25/09	6/25/09	6/25/09

OFFICIAL RECORD COPY