MITSUBISHI HEAVY INDUSTRIES, LTD.
16-5, KONAN 2-CHOME, MINATO-KU
TOKYO, JAPAN

November 14, 2013

Document Control Desk
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001

Attention: Mr. Perry Buckberg

Docket No. 52-021
MHI Ref: UAP-HF-13270

Subject: **MHI's Revised Response to US-APWR DCD RAI No. 750-5675 Question 19-515 (SRP 19)**

References: 1) "Request for Additional Information No. 750-5675 Revision 2, SRP Section: 19 – Probabilistic Risk Assessment and Severe Accident Evaluation," dated April 28, 2011.
2) Letter MHI Ref. UAP-HF-11201 from Y. Ogata to U.S. NRC, "MHI's Responses to US-APWR DCD RAI No. 750-5675 Revision 2 (SRP 19)," dated June 30, 2011.

With this letter, Mitsubishi Heavy Industries, Ltd. ("MHI") transmits to the U.S. Nuclear Regulatory Commission ("NRC") a document entitled "Revised Response to Request for Additional Information No. 750-5675 Question 19-515."

Enclosed is the revised response to Question 19-515 contained within Reference 1. The original response to Question 19-515 was previously submitted to the NRC in Reference 2. The response was revised to address NRC feedback provided during a public meeting on March 28, 2013. This revised response supersedes the previous response.

Please contact Mr. Joseph Tapia, General Manager of Licensing Department, Mitsubishi Nuclear Energy Systems, Inc. if the NRC has questions concerning any aspect of this submittals. His contact information is provided below.

Sincerely,

Yoshiki Ogata,
Executive Vice President
Mitsubishi Nuclear Energy Systems, Inc.
On behalf of Mitsubishi Heavy Industries, LTD.

D081
NRO

Enclosure:

1. Revised Response to Request for Additional Information No. 750-5675 Question 19-515

CC: P. Buckberg
J. Tapia

Contact Information
Joseph Tapia, General Manager of Licensing Department
Mitsubishi Nuclear Energy Systems, Inc.
11405 North Community House Road, Suite 300
Charlotte, NC 28277
E-mail: joseph_tapia@mnes-us.com
Telephone: (704) 945-2740

Docket No. 52-021
MHI Ref: UAP-HF-13270

Enclosure 1

UAP-HF-13270
Docket Number 52-021

Revised Response to Request for Additional Information
No. 750-5675 Question 19-515

November 2013

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

11/14/2013

US-APWR Design Certification

Mitsubishi Heavy Industries

Docket No.52-021

RAI NO.: NO. 750-5675 REVISION 2

SRP SECTION: 19 – Probabilistic Risk Assessment and Severe Accident Evaluation

APPLICATION SECTION: 19

DATE OF RAI ISSUE: 04/28/2011

QUESTION NO. : 19-515

In RAI Questions 19-35 and 19-327 the staff requested additional information about I&C software failures modeled in the PRA, I&C hardware CCF, assumptions regarding diversity and their probabilities and associated uncertainties. MHI responded by performing sensitivity studies, including hardware CCF, and by re-classifying applications software failures into three groups. Groups 1 and 2 impact the safety-related performance and safety monitoring system (PSMS) while Group 3 impacts non-safety related I&C systems. This information was also included in Revision 2 of the DCD. The staff's review identified discrepancies between the provided event definitions and expected results, such as related cut sets (e.g., missing an expected cut set that includes the "transient" initiating event followed by I&C hardware CCF and failure of DAS with a frequency of $1x10^{-8}$ per year) and risk importance values (e.g., expected Group 1 software failure RAW value). The staff followed up with RAI Question 19-428 requesting clarification of the provided definitions of I&C hardware CCF and application software failures. Although in its response MHI provided more detailed information about the treatment of I&C hardware and software CCF in the system analysis, a more precise definition of these basic events is needed, in terms of what signals are impacted by each event.

ANSWER:

Both safety-related digital I&C CCF (hardware and software) and DAS failure will lead to failure of reactor trip. This corresponds to ATWS event and does not appear in the cutset of transient event. Risk importance measures for these failure modes were adequately estimated in the ATWS event.

Definition of basic events regarding digital I&C system is as follows:

Digital I&C hardware CCF (ID: SGNBTHWCCF)

The digital I&C hardware CCF is defined as a hardware failure within the PSMS which consists of RPS (reactor protection system), ESFAS (engineered safety feature actuation system) and SLS (safety logic system). Within the safety-related signals modeled in the US-APWR PRA, only reactor trip signal is generated from the RPS and other signals such as ECCS actuation signal and under voltage signal are generated from SLS through RPS and ESFAS. The hardware CCF results in no actuation of all safety-related signals using PSMS. In addition, operators cannot monitor plant parameters and actuate components using PSMS in the case of hardware CCF. PRA assumes probability of the hardware CCF with 2.1E-06/demand. The hardware CCF probability was evaluated by summing the CCF probabilities of modules and components in RPS, ESFAS and SLS, using the MGL method. The CCF probability of each component and module and a summary are provided in Table 6A.13-8 of the PRA Technical Report (MUAP-07030 Rev.3, Proprietary).

Digital I&C basic software CCF (ID: RTPBTSWCCF)

Basic software CCF is defined as a failure of the MELTAC (Mitsubishi Electric Total Advanced Controller) operation system, which encompasses the common software for PSMS and plant control and monitoring system (PCMS) which is non-safety related I&C system. The basic software failure causes loss of all functions for signals, monitor of plant parameters and actuation of components using digital I&C system for PSMS and PCMS. PRA assumes probability of the basic software CCF with 1.0E-07/demand. The basic software CCF probability was evaluated, assuming one CCF occurs through 20-million-hour operating experience, although no CCF has occurred in MELTAC platform. The 20-million-operating experience was evaluated as follows:

- The MELTAC platform has been in operation since 1987 in Japan.
- Applied to approximately 450 controllers in 30 plants
- Each controller has 2,000 to 200,000 hours operating history (average 8 years)
- MELTAC platform experience was approximately 30 million hours (8,760 hours/year x 8 year 450 controllers) as of February 2011.
- Although MELTAC platform has approximately 30-million-hour operating experience, 20-million-hours operating experience was used for estimation of basic software CCF probability used in the US-APWR PRA.

The detailed basis of the basic software CCF probability is addressed in Chapter 7 of PRA Technical Report (MUAP-07030 Rev.3, Proprietary). Due to the lack of actual CCF events to estimate coupling factors, it was conservatively assumed that additional failures are completely coupled with the second failure.

Application software CCF

Application software of I&C system is different software for PSMS and PCMS. For PSMS, RPS consists of two separate digital controllers to achieve defense-in-depth through functional diversity, as described in DCD Section 7.2.1. Application software of PSMS is divided into two types in the PRA to adequately represent the design feature: one is Group 1 application software and is used for signals generated from SG water level. The other is Group 2 application software and is used for signals generated from parameters other than SG water level. In the PRA model of DCD Rev.3, reactor trip signals, turbine trip signals,

EFW actuation and EFW isolation signals are generated using Group 1 application software. Reactor trip signals, turbine trip signals and signals other than EFW actuation and isolation signals are generated from Group 2 application software. CCFs of the application software are represented as **SGNBTSWCCF1** and **SGNBTSWCCF2**, respectively. Operators cannot monitor the plant parameters and actuate the components using the PSMS. On the other hand, application software for PCMS is represented as **SGNBTSWCCF3**. Operators cannot monitor the plant parameters and actuate the components using the PCMS. PRA assumes that CCF probabilities of PSMS and PCMS are 1.0E-05/demand and 1.0E-04/demand, respectively. The detailed basis of the application software CCF probability is addressed in Chapter 7 of PRA Technical Report (MUAP-07030 Rev.3, Proprietary). As was done for the Digital I&C basic software, it was conservatively assumed that additional failures are completely coupled with the second failure.

MHI will change the concept for modeling the application software CCF. Group 1 application software is used for all signals other than signals to maintain AAC operation discussed below. Due to the design characteristic of the RPS, the reactor trip signals are generated from both Group 1 and 2 application software. The changes will be incorporated in the DCD PRA model. Increase of the CDF reflecting this model change is less than 10% of the internal event CDF reported in DCD Subsection 19.1.4.1.

AAC Actuation Signal

The AACs are designed to minimize the potential CCF with Class 1E GTGs and this design feature is reflected in the digital I&C system for the Class 1E GTGs and AACs.

Class 1E GTGs and AACs automatically actuate upon detection of under-voltage relays on Class 1E ac buses (i.e., A, B, C and D) and non-Class 1E ac buses (i.e., P1 and P2), respectively. Class 1E GTG are automatically actuated upon receipt of the under voltage (UV) signal from the PSMS and the continuous operation is controlled using the PSMS. On the other hand, AACs are automatically started by the UV signal generated from the PCMS and the operation can be maintained using the digital I&C system independent from the MELTAC operation system. Following lists summarizes the basic event modeled in the PRA and the affected failure mode of Class 1E GTGs and AACs.

Reactor Trip Signal

US-APWR PRA considers that the reactor trip signal automatically actuates by detection of either SG water level low or pressurizer pressure high. As described in DCD Section 7.2.1, the RPS consists of two separate digital controllers. Due to the design feature, the reactor trip signals are generated from the application software Groups 1 and 2 and no dependency between the application software CCFs are modeled in the PRA. The signals is generated using the PSMS, therefore, the PSMS hardware CCF (**SGNBTHWCCF**) or basic software CCF (**RTPBTSWCCF**) leads to failure of the reactor trip signal.

Description		Basic Event ID in PRA	Unreliability	Class 1E GTG		AAC	
				Fail to Start	Fail to Run	Fail to Start	Fail to Run
MELTAC Operation System	Basic software CCF	SGNBTHWCCF	1.0E-07	X	X	X	
	Hardware CCF	RTPBTSWCCF	2.1E-06	X	X		
	Application software CCF	SGNBTSWCCF1	1.0E-05	X	X		
		SGNBTSWCCF2	1.0E-05				
		SGNBTSWCCF3	1.0E-04			X	
System Dedicated for AACs	Hardware CCF	EPPBTHWCCF	2.1E-06				X
	Application software CCF	EPPBTSWCCF	1.0E-04				X

Table 19.515-1 shows the automatic signals modeled in the PRA, related I&C system and impact caused by signal failure. CCF of I&C system has impact on all initiating events other than reactor vessel rupture (RVR) event. The US-APWR is designed with DAS to protect against the I&C software CCF discussed above. The DAS function is summarized in DCD Table 7.8-5, and the Level 1 PRA expects the following functions:

(1) Reactor Trip

(2) Turbine Trip

(3) Emergency Feedwater Actuation

(4) Safety Injection Pump

(5) Safety Depressurization Valve

Items (1) and (2) are effective functions to reduce risk caused by ATWS. Item (3) enables the reliability of decay heat removal system via SGs to be higher. Items (4) and (5) can also increase reliability of the core injection system during LOCA events and feed and bleed operation followed by a loss of decay heat removal function using secondary system.

Table 19.515-1 Signals in PRA and Impact Caused by Signal Failure (Updated Table 19.428-3)

#	FT Gate or Basic Event ID	Description	Basic Software	Hardware	Application Software		Impact Caused by Signal Failure	Related System	Related Initiating Event	Remarks
					Gr.1	Gr.2				
1	SGN-SA SGN-SB SGN-SC SGN-SD	ECCS actuation signal	X	X	X	N/A	Failure to start SI pump	High head injection system	All initiating events, excepting, LOCCW, RVR and ATWS	DAS can be expected when I&C CCF occurs.
							Failure to start standby CCW pump	CCWS	All initiating events, excepting, LOCCW, RVR and ATWS	CCW pump start signal (#5) can be also expected.
							Failure to start standby essential chilled water pump	HVAC system	All initiating events, excepting, LLOCA, MLOCA, LOCCW and RVR	HVAC system failure has impact on operability of M/D EFW pump.
							Failure to open motor-operated valve to supply CCW to CS/RHR heat exchanger	CS/RHR system	All initiating events, excepting, LOCCW, RVR and ATWS	
							Failure to start ESW pump	ESWS	All initiating events, excepting, LOCCW and RVR	
2	SGN-PA SGN-PB SGN-PC SGN-PD	Containment spray signal	X	X	X	N/A	Failure to start CS/RHR pump	CS/RHR system	All initiating events, excepting, LOCCW, RVR and ATWS	Operator action can be also expected as recovery (A and C trains only).
							Failure to open containment spray injection line motor-operated valve	CS/RHR system	All initiating events, excepting, LOCCW, RVR and ATWS	Operator action can be also expected as recovery (A and C trains only).
							Failure to close CCW return and supply tie-line valve	CCWS	All initiating events, excepting, LOCCW, RVR and ATWS	Operator action can be also expected as recovery.
3	RTP-MF	Reactor trip	X	X	X	X	Failure of reactor trip	Reactor trip system	All initiating events, excepting LOCA, MLOCA, RVR, LOAC and LODC.	DAS can be expected when I&C CCF occurs. Reactor trip failure results in ATWS event. RPS consists of two groups to achieve diversity within the system.

#	FT Gate or Basic Event ID	Description	Basic Software	Hardware	Application Software		Impact Caused by Signal Failure	Related System	Related Initiating Event	Remarks
					Gr.1	Gr.2				
4	TTP	Turbine trip	X	X	X	N/A	Failure of turbine trip	Turbine trip system	ATWS	DAS can be expected when I&C CCF occurs. Reactor trip and turbine trip failure results in core damage.
5	SGNST-CCWA SGNST-CCWB SGNST-CCWC SGNST-CCWD	Signal to open the normally closed motor-operated valve in the CCW line to provide CCW to the CS/RHR heat exchanger	X	X	X	N/A	Failure to open motor-operated valve to supply CCW to CS/RHR heat exchanger	CS/RHRS (CCWS)	All initiating events, excepting LOCCW, RVR and ATWS	ECCS actuation signal (#1) can be also expected.
6	SGNST-CCWBPL SGNST-CCWDPL	Signal to start the standby CCW pump upon detection of low pressure at the CCW header	X	X	X	N/A	Failure to start standby CCW pump	CCWS	All initiating events, excepting LOCCW, RVR and ATWS	ECCS actuation signal (#1) can be also expected.
7	SGNST-BOA SGNST-BOB SGNST-BOC SGNST-BOD	Signal to start the Class 1E GTGs upon detection of under voltage of its associated Class 1E ac bus	X	X	X	N/A	Failure to start Class 1E GTG	Emergency power supply system	All initiating events, excepting RVR and ATWS	
							Failure to separate RAT	Emergency power supply system	All initiating events, excepting RVR and ATWS	
		Signals to restart the CCW pumps in the loss of offsite power event					Failure to re-start CCW pump in loss of offsite power event	CCWS	All initiating events, excepting LOCCW, RVR and ATWS	
		Signals to restart the ESW pumps in the loss of offsite power event					Failure to re-start ESW pump in loss of offsite power event	ESWS	All initiating events, excepting LOCCW, and RVR	
8	SGNST-BOP1 SGNST-BOP2	Signal to start the AACs upon detection of under voltage of its associated non-Class 1E ac bus	X	N/A	N/A	N/A	Failure to start AAC	Emergency power supply system	All initiating events, excepting RVR and ATWS	AACs are actuated by PCMS and the continuous operation is supported by the digital I&C system dedicated for AACs.
							Failure to separate UAT	Emergency power supply system	All initiating events, excepting RVR and ATWS	

#	FT Gate or Basic Event ID	Description	Basic Software	Hardware	Application Software		Impact Caused by Signal Failure	Related System	Related Initiating Event	Remarks
					Gr.1	Gr.2				
9	SGNST-ISA SGNST-ISB SGNST-ISC SGNST-ISD	Main steam isolation signal	X	X	X	N/A	Failure to close main steam isolation valve	Main steam isolation system (Main steam suppression system)	SLBO, SLBI and FWLB	
		Signals to open the main steam relief valve of the faulted loop					Failure to close main steam relief valve of the faulted loop.	Isolation of faulted SG (Main steam suppression system)	SGTR	
		Signal to open the turbine bypass valves					Failure to open turbine bypass valves	Turbine bypass system (Main steam suppression system)	SGTR	Operator action can be also expected as recovery.
10	SGNST-EFWPA SGNST-EFWPB SGNST-EFWPC SGNST-EFWPD	Signal to isolate EFW supplying to the faulted SG in SGTR event	X	X	X	N/A	Failure to close EFW flow control valve or EFW isolation valve	EFWS	SGTR	
		Signals to start EFW pumps and open T/D EFW pump steam supply line isolation valve					Failure to generate EFW actuation signal	EFWS	All initiating events, excepting LLOCA, MLOCA and RVR	DAS can be expected when I&C CCF occurs.

X: Applicable
NA: Not Applicable

Impact on DCD

Re-quantified PRA results will be reflected in the DCD Chapter 19 after the PRA is revised. If new risk-significant SSCs are identified by the revised PRA results, the SSCs will be incorporated into DCD Table 17.4-1 "Risk-significant SSC".

Impact on R-COLA

The site-specific PRA model will be revised by reflecting the DCD PRA model change and the results will be incorporated in R-COLA Part 2 FSAR Chapter 19 after the DCD PRA model is revised.

Impact on PRA

Digital I&C model for turbine trip, EFW actuation, EFW isolation and AAC actuation signals will be revised to reflect the RAI response when the PRA is revised.

Impact on Topical/Technical Reports

Additional explanation for the CCF based on the 20-million-hour-operating experience will be addressed in PRA Technical Report (MUAP-07030, Proprietary) in the next revision.