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

June 12, 2009

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

Attention: Mr. Jeffrey A. Ciocco

Docket No. 52-021
MHI Ref: UAP-HF-09312

Subject: **MHI's Responses to US-APWR DCD RAI No.364-2655 Revision 1**

References: 1) "Request for Additional Information No. 364-2655 Revision 1, SRP Section: 19 - Probabilistic Risk Assessment and Severe Accident Evaluation, Application Section: 19," dated May 13, 2009.

With this letter, Mitsubishi Heavy Industries, Ltd. ("MHI") transmits to the U.S. Nuclear Regulatory Commission ("NRC") a document as listed in Enclosures.

As indicated in the enclosed materials, this document contains information that MHI considers proprietary, and therefore should be withheld from public disclosure pursuant to 10 C.F.R. § 2.390 (a)(4) as trade secrets and commercial or financial information which is privileged or confidential. A non-proprietary version of the document is also being submitted with the information identified as proprietary redacted and replaced by the designation "[ ]".

This letter includes a copy of the proprietary version (Enclosure 2), a copy of the non-proprietary version (Enclosure 3), and the Affidavit of Yoshiki Ogata (Enclosure 1) which identifies the reasons MHI respectfully requests that all materials designated as "Proprietary" in Enclosure 2 be withheld from public disclosure pursuant to 10 C.F.R. § 2.390 (a)(4).

Please contact Dr. C. Keith Paulson, Senior Technical Manager, Mitsubishi Nuclear Energy Systems, Inc. if the NRC has questions concerning any aspect of the submittals. His contact information is below.

Sincerely,

Y. Ogata

Yoshiki Ogata,
General Manager- APWR Promoting Department
Mitsubishi Heavy Industries, LTD.

Enclosures:

D081
NRO

1. Affidavit of Yoshiki Ogata

2. Responses to Request for Additional Information No. 364-2655 Revision 1 (proprietary version)

3. Responses to Request for Additional Information No. 364-2655 Revision 1 (non-proprietary version)

CC: J. A. Ciocco
C. K. Paulson

Contact Information
C. Keith Paulson, Senior Technical Manager
Mitsubishi Nuclear Energy Systems, Inc.
300 Oxford Drive, Suite 301
Monroeville, PA 15146
E-mail: ck_paulson@mnes-us.com
Telephone: (412) 373-6466

ENCLOSURE 1

Docket No. 52-021
MHI Ref: UAP-HF-09312

MITSUBISHI HEAVY INDUSTRIES, LTD.

AFFIDAVIT

I, Yoshiki Ogata, state as follows:

1. I am General Manager, APWR Promoting Department, of Mitsubishi Heavy Industries, LTD ("MHI"), and have been delegated the function of reviewing MHI's US-APWR documentation to determine whether it contains information that should be withheld from public disclosure pursuant to 10 C.F.R. § 2.390 (a)(4) as trade secrets and commercial or financial information which is privileged or confidential.

2. In accordance with my responsibilities, I have reviewed the enclosed document entitled "Responses to Request for Additional Information No. 364-2655 Revision 1" dated June 2009, and have determined that portions of the document contain proprietary information that should be withheld from public disclosure. Those pages containing proprietary information are identified with the label "Proprietary" on the top of the page and the proprietary information has been bracketed with an open and closed bracket as shown here "[ ]". The first page of the document indicates that all information identified as "Proprietary" should be withheld from public disclosure pursuant to 10 C.F.R. § 2.390 (a)(4).

3. The information identified as proprietary in the enclosed document has in the past been, and will continue to be, held in confidence by MHI and its disclosure outside the company is limited to regulatory bodies, customers and potential customers, and their agents, suppliers, and licensees, and others with a legitimate need for the information, and is always subject to suitable measures to protect it from unauthorized use or disclosure.

4. The basis for holding the referenced information confidential is that it describes the unique design and methodology developed by MHI for performing the design of the US-APWR reactor.

5. The referenced information is being furnished to the Nuclear Regulatory Commission ("NRC") in confidence and solely for the purpose of information to the NRC staff.

6. The referenced information is not available in public sources and could not be gathered readily from other publicly available information. Other than through the provisions in paragraph 3 above, MHI knows of no way the information could be lawfully acquired by organizations or individuals outside of MHI.

7. Public disclosure of the referenced information would assist competitors of MHI in their design of new nuclear power plants without incurring the costs or risks associated with the design of the subject systems. Therefore, disclosure of the information contained in the referenced document would have the following negative impacts on the competitive position of MHI in the U.S. nuclear plant market:

   A. Loss of competitive advantage due to the costs associated with development of methodology related to the analysis.

B. Loss of competitive advantage of the US-APWR created by benefits of modeling information.

I declare under penalty of perjury that the foregoing affidavit and the matters stated therein are true and correct to the best of my knowledge, information and belief.

Executed on this 12nd day of June 2009.

Y. Ogata

Yoshiki Ogata,
General Manager- APWR Promoting Department
Mitsubishi Heavy Industries, LTD.

Docket No. 52-021
MHI Ref: UAP-HF-09312

Enclosure 3

UAP-HF-09312
Docket Number 52-021

Responses to Request for Additional Information
No. 364-2655 Revision 1

June 2009
(Proprietary Information Excluded)

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

6/12/2009

US-APWR Design Certification

Mitsubishi Heavy Industries

Docket No.52-021

RAI NO.: **NO.364-2655 REVISION 1**

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

APPLICATION SECTION: **19**

DATE OF RAI ISSUE: **5/13/2009**

QUESTION NO. : 19-322

Please provide the following information related to your response to RAI Question 19-28:
(a) It is stated that the reactor trip system (RTS) consists of two separate digital controllers to achieve defense-in-depth through functional diversity. However, for the engineered safeguard features (ESF) system, it is stated that "there is no consideration of functional diversity," even though the ESF also includes two different controllers. Please discuss how functional diversity is modeled in the PRA and explain why no functional diversity is considered for the ESF.
(b) Explain how the failure of the power interface (I/F) module, which does not appear in Tables 19.28-1&2, was modeled in the PRA.
(c) It is stated in the response that several components/modules (e.g., CPU power supplies, E/O converters) will be considered during the PRA update. Please discuss how the failure of such components/modules will be modeled and state when the next PRA update is expected.
(d) Discuss how manual actuation signals were modeled in the PRA..

ANSWER:

Response to (a):

For Reactor Trip System, two RPS controller groups per one train have functional diversity processing diverse variables. In PRA, these diverse controller groups don't simultaneously loss their functionality due to application software CCF.

On the other hand, for ESF System, RPS controller groups are not considered to have diversity and application software CCF results in total loss of RPS functions in PRA model.

As functional diversity, ESF System has manual initiation function bypassing automatic actuation part of RPS. However, this is not modeled in PRA since software CCF is dominant.

In addition, SLS per one train has two or three controller groups which process diverse application from each other. However, to simplify Fault Tree model, this functional diversity is not considered in PRA.

Two controllers in ESFAS and SLS in PRA model are parallel redundant controllers which process same application as each other and there is no functional diversity. Application software CCF results in total loss of functions of these redundant controllers.

Response to (b):

The unreliability of power interface module is considered to be factored in the unreliability of each frontline component. Comparison of the reliability between plant component and power interface module is described in the response to RAI 07.1-22 of RAI#229.

However, digital part of power interface module is not covered by frontline component. Therefore, digital part of power interface module will be modeled as part of PSMS in the PRA. The unavailability of the digital part of the power interface module is shown in response to question 19-325. The unavailability of this device will not dominate the unreliability of PSMS so the impact of this model change is small.

Response to (c):

In the response to question 19-28, MHI stated that several components/modules will be modeled in the PRA. The components/modules are listed below along with how those failures will be modeled in the fault tree.

- Power supplies of the RPS for reactor trip function

  The CPU and output part of the RPS are fail safe design and therefore failure of power module will not result in failure of actuating reactor trip signal. Power supply to the CPU and output part of the RPS is therefore not modeled. If power supply to the A/I module, which is the input part of the RPS, losses its function, the RPS cannot read the parameters from sensors. Failures of I/O module power supplies are considered as a cause of A/I module to fail and will be modeled in the fault tree.

- E/O of the processing part of RPS

  A partial trip signal for a given parameter (e.g. steam generator water level, pressurizer pressure) is generated if one trains measurement exceeds it limit. RPS of each train sends its own partial trip signal to each of the other three trains via E/O modules. The RPS generates a trip signal if two or more trains of the same variable are in the same state. In the PRA model for DCD rev.0, communication between RPS trains were not modeled in detail. The PRA will be revised to model all combinations of E/O failures as well as RPS failures that can prevent the RPS to receive two or more partial trip signals.

- E/O of output part of RPS and input part of ESFAS:

  The trip signal from RPS is sent to the each train of the engineered safety feature actuation system (ESFAS) via E/O modules. Each train of the ESFAS receives a trip signal from each of the four RPS trains and processes the signal with a two out of four voting logic and sends the system level ESF actuation signal. The failure of E/O modules can prevent the ESF to receive trip signals from RPS Failure of these E/O modules will be considered in the fault tree as a cause of ESFAS failing to receive trip signals from the associated RPS train.

- Distribution module of output part of SLS

  Distributor failure of the output part of the SLS will result in failure of ESF actuation signal to each component. Since this failure will result in component level failure, this failure mode was excluded from the boundary of SLS. Failure of distributor will result in failure of each component to actuate. The distributor is simple static equipment with low failure rate, expected to be orders of 1E-8 /hr, and can be check during surveillance testing. The failure probability of distributor is significantly lower than active components such as valves and pumps, and therefore will not be modeled.

The results of the PRA reflecting these model changes will be shown in the DCD tracking report that will be submitted two to three months from now.

Response to (d):

The PRA takes credit of two kinds of manual actuation signals, (1) safety injection signal and (2) containment spray actuation signal. Manual actuation signals credited in the PRA are described below.

(1)Safety injection signal

When safety injection signal fails due to common cause failure in the RPS or SFS, the operators manually actuate safety injection signal by diverse actuation system (DAS).

(2)Containment spray actuation signal

When containment spray actuation signal fail due to containment pressure sensors, operators manually actuate the containment spray signal by ESFAS.

For the failure to actuate manual signals, two types of causes, human error and software failure, were modeled in the fault tree. Human error is a dominant contributor of single failure because of its relatively large failure probability. Software failure was modeled to take into account dependency.

<u>Impact on DCD</u>

Results of the revised PRA will be reflected to the DCD. Changes to the DCD will be shown in the DCD tracking report.

<u>Impact on COLA</u>

No impact on COLA.

<u>Impact on PRA</u>

The PRA model will be updated. And the results of the PRA will be reflected to the DCD. Detailed description of the model change will be documented in the PRA report.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

6/12/2009

US-APWR Design Certification

Mitsubishi Heavy Industries

Docket No.52-021

RAI NO.: **NO.364-2655 REVISION 1**

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

APPLICATION SECTION: **19**

DATE OF RAI ISSUE: **5/13/2009**

QUESTION NO. : 19-323

Please provide the following information related to your response to RAI Question 19-29:
(a) Discuss how the alternate ac (AAC) power signal is diverse from all other application signals and how the implementation of this diversity will be verified in the as-to-be-built, as-to-be-operated plant (e.g., through an ITAAC). Is this diversity with respect to both hardware and software?
(b) It is stated that a sensitivity study was performed to investigate the impact of complete dependency among all application software, except for AAC, on the PRA results. Please discuss the assumptions made in this sensitivity study. For example, was the same basic event designator assumed for all applications software but the one for AAC actuation? Explain the result of the sensitivity study (i.e., no impact on CDF) in terms of failed equipment and accident sequences involved. Discuss whether this result could be significantly different if the software failure probability was not assumed to be so low.
(c) How was the failure of sensors for the "other" signals (e.g., signal to start the standby component cooling water pumps) considered in the PRA?
(d) Are all "other" signals also generated by the diverse actuation system (DAS)?

ANSWER:

(a)

Application software of non-safety GTG (AAC) start signal is diverse from other signals of ESFAS, while same platform (MELTAC) is used.

In addition, platform different from METAC is used for the control system of AAC. Therefore, even if the AAC does not automatically actuate because of CCF in MELTAC, the AAC can be started manually when connecting to the class 1E bus in the event of station blackout.

Diversity of AAC control system will be verified through ITAAC in DCD Chapter 8, included in verifying diversity of AAC itself, which is diverse from Class 1E GTG.

(b)

In the sensitivity study to investigate the impact of complete dependency among all application software the same basic event was applied to all applications software, except for that of AAC. This model change allows all signals, except for AAC and reactor trip and DAS, to fail with a probability of 1.0E-5. Support software CCF was modeled as it was in the base case.

Cut sets and accident scenario that will dominate the impact of the above assumption are the followings:

(LOFW) x (Application software CCF) x (DAS failure) = 1.9E-8 /RY

> Loss of feed water initiating event followed application software failure and DAS failure. In this scenario, EFW is unavailable since EFW actuation cannot be initiated neither by EFSAS nor DAS and therefore SG cooling cannot be performed. Feed and bleed cannot be performed since safety injection pump and pressurizer safety depressurization valve (SDV) cannot be operated due to application software failure in the safety digital I&C system.

(TRAN) x (Application software CCF) x (DAS failure) x (Fail to recover main feed water) = 8.0E-9 /RY

> General transient initiating event followed application software failure, DAS failure and main feed water recovery. In this scenario, EFW is unavailable since EFW actuation cannot be initiated neither by EFSAS nor DAS. Operation to recover main feed water also fails and SG cooling is unavailable. Feed and bleed cannot be performed since safety injection pump and pressurizer safety depressurization valve (SDV) cannot be operated due to application software failure in the safety digital I&C system.

(LOOP) x (Application software CCF) x (Fail to perform alternate CCW) = 4.0E-9 /RY

> Loss of offsite power followed by application software failure and alternate CCW failure. In this scenario, CCW pump fail to restart due to application software failure. Operation to establish alternate CCW also fails and RCP seal injection is lost. Since the RCP thermal barrier is also unavailable RCP seal LOCA will occur. Safety injection cannot be performed since CCW is lost.

These accident scenarios appear in the cutsets when application software CCF is modeled as a single basic event. The CDF values shown above along with the cutsets are results obtained when application software CCF probability is assumed to be 1.0E-5. When this probability of 1.0E-5 is assumed, these cutsets still do not dominate the CDF. However if software CCF probability were assumed to be significantly higher than 1.0E-5, these cutsets will be the dominant contributors to CDF. Therefore, if the probability of application software CCF were assumed to be higher in the sensitivity analysis in 19-29, results would have been different. Response to question 19-35 shows sensitivity studies assuming the CCF probability of failing all signals, except AAC, to be high up to 1.0E-4.

Software reliability will be documented of key source of uncertainty in the DCD. Sensitivity study on the reliability of software CCF will be documented in the DCD as well.

(c)

Sensor failures for each of the “other signals” were not explicitly modeled. The failure probability applied to “other signals” is considered to include the contribution of sensor failure. This is because the failure probability of other signals, which is equal to the failure probability of containment spray signal, includes the contribution of sensor failure. It should also be noted that “other signal” do not rely on the same sensors in the same accident scenario.

(d) The only “other signal” that takes credited of DAS is the EFW start signal. The PRA takes credit of DAS for the following signals.

- EFW start signal (Automatic)
- Reactor trip signal (Automatic)
- Safety injection signal (Manual)

Impact on DCD

Discussion on sensitivity study in of digital I&C reliability will be added in the chapter 19.1 of the DCD. Page 19.1.38 will be amended as follows.

“

Analysis has been performed to determine the sensitivity of CDF to the following:

- On power maintenance
- Human error rate
- Gas turbine generator reliability
- Digital I&C reliability
- Design and operation

“

Page 19.1.38 will be amended as follows.

“

Digital I&C reliability

Sensitivity analysis of digital I&C software reliability is performed to study the impact of its uncertainty on plant CDF for internal initiating events at power.

- CASE 09 Common cause failure application software
  In this sensitivity analysis, CCF probability of application software used for all signals, except AACs, were given a higher value than the base case. If the probability of application software were assumed to occur with a probability of 1E-4, the resulting CDF will be 1.7E-6 /RY which is 1.5 times higher than the base case.

“

Table 19.1-35 “Key Sources of Uncertainty and Key Assumptions (Level 1 PRA for Internal Events at Power)” will be revised to include uncertainty of digital &C software failure probability.

Impact on COLA

No impact on COLA.

Impact on PRA

No impact on PRA.

Table 19.1-35 Key Sources of Uncertainty and Key Assumptions (Level 1 PRA for Internal Events at Power) (Sheet 3 of 4)

Key Sources of Uncertainty and Key Assumptions		Type (Note)	Summary Results of Qualitative Assessments	Quantitative Approach
Data Analysis	Failure probability and failure rates for diesel generators are applied to gas turbine generators.	M	Sensitivity analysis of failure probability and failure rates was performed.	Sensitivity Analysis (Case 8)
	Statistical uncertainty of failure rate	P	(Statistical uncertainty is considerable)	Uncertainty Analysis
	Failure probability of digital I&C software	M	Sensitivity analysis of failure probability was performed.	Sensitivity Analysis (Case 9)
Common Cause Failure Analysis	CCF parameters of emergency diesel generators are applied to gas turbine generators.	M	Sensitivity analysis of gas turbine generator CCF parameters was performed.	Sensitivity Analysis (Case 07)
	CCF of inter-systems is not included in the CCF model.	M	The environment, operation or service, design, and maintenance are different between inter-systems.	NA
	Statistical uncertainty of CCF probabilities.	P	(Statistical uncertainty is involved in data base)	Uncertainty Analysis

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

6/12/2009

US-APWR Design Certification

Mitsubishi Heavy Industries

Docket No.52-021

RAI NO.: **NO.364-2655 REVISION 1**

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

APPLICATION SECTION: **19**

DATE OF RAI ISSUE: **5/13/2009**

QUESTION NO. : 19-324

Please provide the following information related to your response to RAI Question 19-30:
(a) It is stated that hardware CCF is not modeled for I&C systems because it is not significant. Table 19-30-1 of the response, reports an estimate of the ESF system hardware CCF as 4E-6. It is argued that hardware CCF is not significant since the ESF system hardware CCF probability (4E-6) is smaller than the application software failure probability (1E-5). However, these two probabilities are roughly of the same order of magnitude, especially when the associated uncertainties are considered. Furthermore, the modeling of the CCF of I&C hardware in the PRA is important for importance and sensitivity analyses as well as for risk-informed applications. Please discuss.
(b) Provide the basis for the very low component unavailability and discuss how the CCF of sensors and power interface modules was considered.

ANSWER:

(a)

Hardware CCF of digital I&C system will be modeled in the PRA. Hardware CCF that results in failure of all four trains of the signal system will be modeled as a basic event that counts for the total CCF probabilities. CCF of the I&C system hardware that results in failure of protection and safety monitoring system (PSMS) was reevaluated, taking into account the update of I&C hardware availability, and are estimated to be 2.2E-6.

CCF probabilities of each digital I&C hardware that result in failure of all signal trains are shown in table 1.

Following assumptions were made during the estimation of I&C hardware CCF probability.

- Failure rates used for estimation of single component unavailability are applied. The equation used to calculate the availability of I&C system are the same, but the some parameters (MTTR and SDR) have been adjusted for the purpose of calculating hardware CCFs.
- The mean time to repair (MTTR) is set to be 6 hours. This is because CCF among trains in the PSMS will violate LCO and the plant will be shutdown within 6 hours.
- Self diagnosis rate (SDR) of I&C hardware is set 100% for hardware CCFs. CCF of I&C hardware occurs when CCF of the device, which provides the mitigation function. Its self diagnosis function can detect the hardware failures, and loss of self diagnosis function of all CPUs in conjunction with hardware CCF of mitigation function is not likely to occur. Therefore, SDR is set 100% for hardware CCFs.
- MGL parameters applied for I&C hardware are consistent with those described in response to question 19-30. The MGL parameters for CCF of 5th component and greater are set to 1.0.

This model change will result in increase of CCF probability of signals. Increase of the CCF probability if signal is 25% of the probability of application software CCF, which has same impact to the signals. Sensitivity studies discussed in response to question 19-35 show that CDF increased only 1.1 times when application software CCF probability was set a factor of two higher than the base case. This implies that the increase in CDF resulting from this model change, which has smaller impact than the sensitivity case in response to 19-35; is considered to be small.

(b)

CCFs of sensors were modeled as basic events. CCFs of power interface module were considered to be covered by the CCF probabilities of frontline components. The unreliability of power interface module is considered to be factored in the unreliability of frontline components. And CCF of power interface module is also considered to be factored in the CCF probabilities of frontline components as well when CCF of frontline components are quantified. Comparison of the reliability between plant component and power interface module is described in the response to RAI 07.1-22 of RAI#229.

Digital part of power interface module is not covered by frontline component. Therefore, digital part of power interface module will be modeled as part of PSMS in the next revision of PRA Technical Report.

Impact on DCD

Results of the revised PRA will be reflected to the DCD. Changes to the DCD will be shown in the DCD tracking report. Impact to the results of the PRA is small.

Impact on COLA

No impact on COLA.

Impact on PRA

The PRA model will be updated and the results will be reflected to the DCD. Detailed description of the model changes will be documented in the PRA report. Impact to the results of the PRA is small as discussed in the answer to the question.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

6/12/2009

US-APWR Design Certification

Mitsubishi Heavy Industries

Docket No.52-021

RAI NO.: **NO.364-2655 REVISION 1**

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

APPLICATION SECTION: **19**

DATE OF RAI ISSUE: **5/13/2009**

QUESTION NO. : 19-325

In the response to RAI Question 19-33 it is stated that the failure probability for each module type was estimated from the failure rates of the devices that compose the module, through a failure and effects analysis (FEA). It is also stated that the potential for detecting (self diagnosis) and repairing failed modules was considered. Please provide a list of failure and failure detection rates for each module modeled in the PRA as well as more detailed information regarding their basis.

ANSWER:

Self-diagnosis function and its checking failure of MELTAC platform is described in Topical Report MUAP-07005 Section 4.1.5.1 and diagnosis coverage is 100%. However, self-diagnosis rate is conservatively considered to be 90% in PRA for failure rate calculation of each digital module, considering failure of self-diagnosis itself. Parameters used to estimate unavailability of each modules used for reactor trip signal and engineered safety feature actuation signal are shown in table 1 and table 2.

Impact on DCD

No impact on DCD.

Impact on COLA

No impact on COLA.

Impact on PRA

No impact on PRA.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

6/12/2009

US-APWR Design Certification

Mitsubishi Heavy Industries

Docket No.52-021

RAI NO.: NO.364-2655 REVISION 1

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

APPLICATION SECTION: 19

DATE OF RAI ISSUE: 5/13/2009

QUESTION NO. : 19-326

Please provide the following information related to your response to RAI Question 19-34:
(a) It is stated that digital I&C room cooling is not modeled because the HVAC system is normally operating and therefore the probability to fail within the 24-hour mission time is small. However, the staff notes that according to Section 6A.14.4.1.3 of the PRA report on "Instrumentation and Control," the HVAC fans are in standby during normal operation, which implies that failure to start must also be modeled in the PRA. In addition, the staff notes that the failure to run rate of fans is in the range of 1E-3 to 1E-4 per hour, which does not appear to be negligible. Please discuss.
(b) Discuss how the failure of HVAC is detected during normal plant operation and what requirements are in place to ensure that the plant is not operating w/o room cooling for extended time intervals. Provide the basis (e.g., a combination of analysis and supporting arguments) indicating that the lack of modeling of loss of I&C room cooling in the PRA does not impact the PRA results and insights.

ANSWER:

Answer to item (a)

The HVAC fans of class 1E electrical rooms, which provide air to I&C room, are normally running. Description in the PRA report will be amended.

Taking into consideration that failure to start on demand are the dominant causes of safeguard components to fail, it is reasonable to make an engineering judge that the reliability of normally operating HVAC to have relatively higher reliability than frontline system. The staff is correct that the HVAC fans can fail and such probability cannot be neglected. However, what will impact the risk is simultaneous failures of redundant components in the system that occur within a short period of time, including common cause failures, and lead to functional failure of multiple trains. It is obvious that such simultaneous failures are likely to occur upon components that start at once on demand, rather than components that are normally running and are not required to change its state simultaneously.

Moreover, the 24 mission time is set based on the mission time of frontline systems. However, actuation signals of all trains will actually complete within a short time after the occurrence of an initiating event. Therefore, HVAC of I&C room may not actually be required to be operable for 24 hours. Even if HVAC function were to have impact on signals, they will be limited to those that are required to operate hours after the initiating event. From this point of view, we consider it is a reasonable engineering judgment to assume that the possibility of simultaneous failures in redundant trains of the Class 1E HVAC is negligible compared to failures of frontline systems that are in standby.

Answer to item (b)

Each Digital I&C room is cooled by Class 1E electrical room HVAC system. Failure of Class 1E electrical room HVAC can be detected by either of the following alarms that actuate in the MCR.

- Alarm on Class 1E electrical room high temperature
- Alarm on Class 1E electrical room air handling unit outlet flow rate

Failure of HVAC system necessary for the operability of safety related systems impact not only the mitigation function after occurrence of initiating events but also may cause an initiating event. For instance, a system essential for the plant to be operating, not limited to safety related systems, may lose its function due to loss of HVAC, if the system is dependant on the HVAC. Or, the loss of HVAC may cause spurious actuation of safeguard components that are in standby and cause plant trip. In the former case, since safety related system and non-safety related system do not principally share HVAC systems, failure of non-safety HVAC system that may cause plant trip will not impact the function of safety related systems. Regarding safety related system that are essential for plant operation such as CCWS and ESWS, if losses of HVAC cause degradation of its function, loss of HVAC may cause an initiating event. However, even though losses of "component cooling" of CCW pumps and ESW pumps may cause such an initiating event, it is unlikely for losses of HVAC of the digital I&C room to initiate a CCW or ESWS pump to trip. Similarly, it is unlikely for losses of HVAC to actuate spurious signal and lead to functional failure of system. For these reasons, the possibility of such events to occur is considered to be insignificant, even if losses of HVAC can potentially to lead to failure of mitigating functions or cause an initiating event.

Even though we judge that the probability of losses of Class 1E electrical room HVAC is negligible in PRA, it is obvious from PRA perspective that if losses of Class 1E electrical room HVAC were to occur, and the event impacts components in the most undesirable way, the consequences will be severe. This insight will be documented in the DCD as risk insights and key uncertainties.

Under loss of HVAC, operator action such as opening of room doors and utilizing portable fans can be expected to relax room heat up. The PRA does not explicitly credit for these actions, but since our treatment of class 1E electrical room HVAC has uncertainty, insight that these actions are desirable when losses of HVAC occur will be documented in the DCD and define a COL item to consider such actions.

Impact on DCD

Table 19.1-35 and 19.1-115 will be revised.

Table 19.1-35 Key Sources of Uncertainty and Key Assumptions (Level 1 PRA for Internal Events at Power)

Key Sources of Uncertainty and Key Assumptions		Type (Note)	Summary Results of Qualitative Assessments	Quantitative Approach
				NA
Success Criteria Analysis	Boundary conditions Plant parameters	M	Appropriate simplified evaluations for the US-APWR have been performed.	NA
System Analysis	Plugging before events occurred is not modeled.	M	It would be hard to plug during normal operation in RCS and safety related systems.	NA
	System unavailability	M	US generic data is considered appropriate at design stage. However, Sensitivity analyses were performed.	Sensitivity Analysis (Case 1, Case 2)
	Class 1E electrical room HVAC are reliable and do not impact risk	M	Even if losses of HVAC occur, actuation signals of all trains will actually complete within a short time after the occurrence of an initiating event, and therefore, losses of HVAC may not affect the signal actuation. Even if HVAC function were to have impact on signals they will be limited to those that are required to operate hours after the initiating event. It is unlikely for losses of HVAC to actuate spurious signal and lead to functional failure of system so HVAC failure are likely to cause plant trip or malfunction of operating mitigation systems. To relax room heat up after losses of Class 1E electrical room HVAC, the operator will be open the room door and utilize available portable fans.	If Class 1E electrical room heat up were to occur and impact components in the most undesirable way, conditional core damage frequency will be 1.0 and the consequences will be severe.

Table 19.1-115 Key Assumptions (Sheet 1 of 4)

Key assumptions
Operator actions Operator actions modeled in the PRA are based on symptom oriented procedures. Risk significant operator actions identified in the PRA will be address in the EOP. If losses of Class 1E electrical room HVAC occur, operator will be open the room door and utilize available portable fans to relax room heat up. This operator action will be disposition in severe accident manage program (19.2.5). **Operator actions during at power events** a. In the case of loss of CCW event, operators will connect the non-essential chilled water system or the fire suppression system to the CCWS in order to cool the charging pump and maintain RCP seal water injection. b. If emergency feed water pumps cannot feed water to two intact SGs, operators will attempt to open the cross tie-line of EFW pump discharge line in order to feed water to two more than SGs by one pump. c. The CS/RHR System has the function to inject the water from RWSP into the cold leg piping by switching over the CS/RHR pump lines to the cold leg piping if all safety injection systems failed (Alternate core cooling operation). Alternate core cooling operation may be required under conditions where containment protection signal is valid. In such cases, alternate core cooling operation is prioritized over containment spray, because prevention of core damage would have higher priority than prevention of containment vessel rupture.

Impact on COLA

No impact on COLA.

Impact on PRA

No impact on PRA.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

6/12/2009

US-APWR Design Certification

Mitsubishi Heavy Industries

Docket No.52-021

RAI NO.: **NO.364-2655 REVISION 1**

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

APPLICATION SECTION: **19**

DATE OF RAI ISSUE: **5/13/2009**

QUESTION NO. : 19-327

In the response to RAI Question 19-35 it is stated that sensitivity studies were performed to address the uncertainty associated with the assumed probabilities for support and application software failure (1E-7/demand and 1E-5/demand, respectively). The staff believes that the assumed probability values in the sensitivity analysis need to be further increased to bound the associated uncertainties and gain a better understanding of the impact of software failure on the PRA results. Also, the digital I&C software failure probabilities should be tracked as an area of uncertainty to be taken into account when the PRA is used for decision making in risk-informed applications.

ANSWER:

Software CCF assumption of MHI is consistent with those of NEI White Paper entitled “Modeling of Digital I&C in Nuclear Power Plant Probabilistic Risk Assessment” (ML0723350195). NEI White Paper mentions operating experience and important defensive measures, and provides appropriate value of software CCF. For OS (support software), MELTAC platform is implemented with the many defensive measures (such as strictly cyclic operation, constant loading of communication and processing buses,, static memory allocation and asynchronous operation, etc). On these bases, it is appropriate to use 1E-07[/d] as support software CCF considering 20 billion operating experience. In addition, safety-related application software is managed on life cycle process including validation and verification as Class 1E, and is implemented with many defensive measures. On these bases, it is appropriate to use 1E-05 as application software CCF, as shown in NEI White Paper.

The staffs comment is correct that the probability of digital I&C software failure has a large uncertainty. MHI will document the reliability of digital I&C software as a source of uncertainty in DCD chapter 19.

Support software CCF has impact on the CDF of ATWS scenario. The contribution of ATWS events to the total CDF is small, and therefore, impact of support software on the total CDF is small for ATWS events. Support software CCF also causes failure of mitigation systems required for events other than

ATWS. Impact of support system on such mitigation features have similar impact with application software, which now is assumed to result in failure of all safety related signal. Since support software CCF can be considered to have lower probability than application software CCF, the uncertainty of support software CCF probability will have less impact to the total CDF compared to the uncertainty of application software CCF.

Impact on DCD

Discussion on sensitivity study in of digital I&C reliability will be added in the chapter 19.1 of the DCD. Page 19.1.38 will be amended as follows.

“

Analysis has been performed to determine the sensitivity of CDF to the following:

- On power maintenance
- Human error rate
- Gas turbine generator reliability
- Digital I&C reliability
- Design and operation “

Page 19.1.38 will be amended as follows.

“

Digital I&C reliability

Sensitivity analysis of digital I&C software reliability is performed to study the impact of its uncertainty on plant CDF for internal initiating events at power.

- CASE 09 Common cause failure application software
  In this sensitivity analysis, CCF probability of application software used for all signals, except AACs, were given a higher value than the base case. If the probability of application software were assumed to occur with a probability of 1E-4, the resulting CDF will be 1.7E-6 /RY which is 1.5 times higher than the base case.

“

Table 19.1-35 “Key Sources of Uncertainty and Key Assumptions (Level 1 PRA for Internal Events at Power)” will be revised to include uncertainty of digital &C software failure probability.

Table 19.1-35 Key Sources of Uncertainty and Key Assumptions (Level 1 PRA for Internal Events at Power)

Key Sources of Uncertainty and Key Assumptions		Type (Note)	Summary Results of Qualitative Assessments	Quantitative Approach
Data Analysis	Failure probability and failure rates for diesel generators are applied to gas turbine generators.	M	Sensitivity analysis of failure probability and failure rates was performed.	Sensitivity Analysis (Case 8)
	Statistical uncertainty of failure rate	P	(Statistical uncertainty is considerable)	Uncertainty Analysis
	Failure probability of digital I&C software	M	Sensitivity analysis of failure probability was performed.	Sensitivity Analysis (Case 9)
Common Cause Failure Analysis	CCF parameters of emergency diesel generators are applied to gas turbine generators.	M	Sensitivity analysis of gas turbine generator CCF parameters was performed.	Sensitivity Analysis (Case 07)
	CCF of inter-systems is not included in the CCF model.	M	The environment, operation or service, design, and maintenance are different between inter-systems.	NA
	Statistical uncertainty of CCF probabilities.	P	(Statistical uncertainty is involved in data base)	Uncertainty Analysis

Impact on COLA

No impact on COLA.

Impact on PRA

No impact on PRA.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

6/12/2009

US-APWR Design Certification

Mitsubishi Heavy Industries

Docket No.52-021

RAI NO.:	**NO.364-2655 REVISION 1**
SRP SECTION:	**19 – Probabilistic Risk Assessment and Severe Accident Evaluation**
APPLICATION SECTION:	**19**
DATE OF RAI ISSUE:	**5/13/2009**

QUESTION NO. : 19-328

In the response to RAI Question 19-36 it is stated that different application software are installed in the two separate digital controllers of each train of the reactor protection system (RPS) and, therefore, the software failure will fail only one controller per train. Please explain how these application software are different for the two controllers. Are
they diverse? Also, it is stated that "application software failure for each digital controller will be modeled and the sensitivity will be studied" during the PRA update for RMTS Initiative 4b. Is this a COL action item? Please clarify.

ANSWER:

For Reactor Trip System., two RPS controller groups per one train process diverse variables and these controllers application is diverse from each other. Please refer to response to Question 19-322 for detail.

For ESF System, there is no consideration of functional diversity of variables. As functional diversity, ESF System has manual initiation function and SLS has diverse controller groups, but these diversity is not considered in PRA. Please refer to response to Question 19-322 for detail.

PRA to support RMTS will model address the sensitivity of the following application software.

- RPS #1 application software CCF
- RPS #2 application software CCF
- ESFAS application software CCF
- SLS application software CCF

This PRA upgrade will be part of the licensing of RMTS, which is a part of RMTS licensing issue.

Impact on DCD

No impact on DCD.

Impact on COLA

No impact on COLA.

Impact on PRA

No impact on PRA.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

6/12/2009

US-APWR Design Certification

Mitsubishi Heavy Industries

Docket No.52-021

RAI NO.: NO.364-2655 REVISION 1

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

APPLICATION SECTION: 19

DATE OF RAI ISSUE: 5/13/2009

QUESTION NO. : 19-329

In the response to RAI Question 19-38 it is stated that although two different designators were used for the CCF of the pressurizer pressure sensors basic event, it was judged to have a small impact on the PRA results. The staff review finds that even though the two different designators do not appear to have an impact on the results (since the current ATWS event tree model does not credit any mitigating systems, such as high head injection and emergency feedwater), this may not be the case when a more detailed model is developed in the future. Also, this issue may become significant in sensitivity studies where higher application software failure probabilities are used. Please discuss.

ANSWER:

The fault tree will be revised so that the common basic event will be used for the CCF of the pressurizer pressure sensors. This change will be incorporated in the PRA model. In addition, the ATWS event tree will be revised to model the mitigation system in detail. This PRA model change will be reflected in the DCD tracking report that will be submitted two to three months from now.

For loss of feed water event, which is one of the most severe initiating event for ATWS, reactor trip signal is initiated either by high pressurizer pressure or low steam generator water level. Due to the diversity of input parameters, the probability of reactor trip failure caused by sensor CCF is very low. Even though failure of sensors of diverse plant variables (such as pressurizer pressure and SG water level) can degrade the reliability of both reactor trip signal and engineered safety function actuation signals, the probability of such combination of failures is very low, and such failures would not dominate the CDF for ATWS. Taking into consideration that ATWS has small contribution to the total CDF in the current PRA, it is considered that the model change will not have impact to the CDF.

Impact on DCD

No impact on DCD.

Impact on COLA

No impact on COLA.

Impact on PRA

The PRA will be revised. Changes to the PRA will not have impact on the base results.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

6/12/2009

US-APWR Design Certification

Mitsubishi Heavy Industries

Docket No.52-021

RAI NO.: NO.364-2655 REVISION 1

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

APPLICATION SECTION: 19

DATE OF RAI ISSUE: 5/13/2009

QUESTION NO. : 19-330

In the response to RAI Question 19-39 it is stated that the FV importance of the "failure of the SG isolation signal" event is very low and, therefore, this event does not need to be modeled in the PRA. The staff believes that the FV importance should be considered together with the RAW importance measure to determine risk significance.
Please discuss.
Also, input is provided to DCD Ch. 17.4 in terms of "failure of signal" (e.g., failure of the SG isolation signal)." How will this information be interpreted and used in the reliability assurance program (RAP) of a future plant? The RAP requires a list of SSCs. Is the provided PRA input to Chapter 17.4 related to both the software and hardware portions of a signal? Please clarify in both the PRA and the DCD..

ANSWER:

The staffs comment is correct that the FV importance should be considered together with the RAW importance measure to determine risk significance. The intent of MHI's response to question 19-39 was that deleting the common cause failure (CCF) of "failure of the SG isolation signal", which was incorrect to model, will have negligible impact on the results. The CCF of "failure of the SG isolation signal" does not need to be modeled because this signal is required only for the loop which SGTR has occurred, and CCF across trains (or loops) is unnecessary to be considered for this signal. The single failure of "failure of the SG isolation signal" will be modeled. Single failure of "SG isolation signal" are risk important, and it will be listed in the list of risk important SSCs.

Please refer RAI No.175, question 17-04-38, which discusses how signals will be handled in the RAP. The list of risk important SSCs will list the SSCs related to signals, not the signal itself.

Impact on DCD

No impact on DCD.

Impact on COLA

No impact on COLA.

Impact on PRA

No impact on PRA.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

6/12/2009

US-APWR Design Certification

Mitsubishi Heavy Industries

Docket No.52-021

RAI NO.: NO.364-2655 REVISION 1

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

APPLICATION SECTION: 19

DATE OF RAI ISSUE: 5/13/2009

QUESTION NO. : 19-331

In the response to RAI Question 19-40, the second part of the question was not addressed (i.e., explain the basis of the assumed CCF probabilities for the "SG isolation signal"). Please explain.
Also, even though in the response to Question 19-39 it is stated that the event "SG isolation signal CCF" was not supposed to be modeled in the PRA, the response to RAI Question 19-40 implies otherwise. Please clarify.

ANSWER:

Treatment of CCF of signals including "other signals" will be changed. The "CCF-Group" function of the PRA code "Riskspectrum" describe in response to 19-40 will not be used to model CCF between signals. Instead, CCF will be modeled by basic events that represent CCF of signals. For all signals that rely on the protection and safety monitoring system (PSMS), three types of common cause failures, application software CCF, support software CCF and I&C hardware CCF will be considered and modeled as basic events in the fault trees.

Application software CCF can occur upon all engineered safety feature (ESF) signals (e.g. safety injection signal, containment spray signal and "other signals") that use the software of the PSMS and cause failure of all signals with a probability of 1E-5. Support software CCF can occur upon all signals modeled in the PRA and cause failure of all the signals with a probability of 1E-7. I&C hardware CCF can occur upon all signals that use the PSMS and cause failure of all signals with a probability of 2.5E-6. The basis of I&C hardware CCF probability is shown in response to question 19-324.

Thus CCF between trains of the same signal and CCF between different signal that rely upon PSMS will be modeled to take into account CCF caused by software and I&C hardware.

This model change will increase the probability of CCF of signals related to the PSMS.As it is discussed in response to item (a) of question 19-323, impact of this model change on the CDF is small.

Impact on DCD

No impact on DCD.

Impact on COLA

No impact on COLA.

Impact on PRA

The PRA model will be updated and the results will be reflected to the DCD. Detailed description of the model changes will be documented in the PRA report. Impact to the results of the PRA is small as discussed in the answer to the question.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

6/12/2009

US-APWR Design Certification

Mitsubishi Heavy Industries

Docket No.52-021

RAI NO.: NO.364-2655 REVISION 1

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

APPLICATION SECTION: 19

DATE OF RAI ISSUE: 5/13/2009

QUESTION NO. : 19-332

In the response to RAI Question 19-42 it is stated that there are shared sensors and distribution modules between the diverse actuation system (DAS) and the protection and safety monitoring system (PSMS). Please explain how these dependencies are modeled in the PRA.
Also, explain how the assumed reliability/availability goal of 1E-2 per demand will be verified.

ANSWER:

Shared portion between Diverse Actuation System (DAS) and Protection and Safety Monitoring System (PSMS) is sensors and distribution modules. These shared portions are not modeled in current PRA, and so these subsidarities will be included in next revision of PRA model. Impact of this model change to the CDF is small. Since signals that are initiated by DAS and PSMS rely on diverse variables, CCF of one series of sensors will not directly result in failure of actuating a signal. Combination of CCFs that occur on two diverse sensors may result is failure of both DAS and PSMS but such events have very low probabilities. CCF of distribution model also has a very low probability as shown in table 1 of response to question 19-324.

In addition, actuation function of plant component (except of Reactor Trip) from DAS shares also PIF module of PSMS. This is appropriately modeled in current PRA. The consideration of PIF in the PRA is described in response to question 19-322 item (b).

Functional and device configuration of DAS is described below and the simplified diagram is shown in figure 1.

DAS is input with sensor signals from PRS via distribution module and isolation module. Sensor and distribution module is the shared portion between DAS and PSMS. DAS reliability is considered for the portion downstream of isolation module up to MG-set trip.

DAS has two subsystems of Diverse Automatic Actuation Cabinet (DAAC). Each DAAC has four bistable modules (including channel test module) and two redundant logic circuits (Universal logic module, timer module, DC controller module and output relay). Output relay is designed to be energized to actuate.

Reactor Trip signal output from each DAAC opens each field current circuit of two MG set via buffer relay, respectively. Opening of field current circuit results in stop of MG-set generation.

There are two MG-set and one MG set can provide sufficient power for control rod drive mechanism (CRDM). Therefore, both two outputs from each DAAC are required for reactor trip from DAS.

[Unavailability of DAS Reactor Trip]

Unavailability of DAS reactor trip can be evaluated by the fault tree shown in figure 2.

All module unavailability is calculated from MIL based failure rate, considering surveillance frequency and completion time to restore consistent to Technical Specification. Common cause failure probability was estimated using the MGL parameters for I&C components described in response to question 19-30. The resulting unavailability of DAS reactor trip is 6.7 E-3. Thus, the 0.01 unavailability applied for DAS is a bounding value.

Impact on DCD

No impact on DCD.

Impact on COLA

No impact on COLA.

Impact on PRA

The PRA will be revised to consider the shared portion of DAS and PSMS. The impact of this model change to the CDF is small.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

6/12/2009

US-APWR Design Certification

Mitsubishi Heavy Industries

Docket No.52-021

RAI NO.: NO.364-2655 REVISION 1

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

APPLICATION SECTION: 19

DATE OF RAI ISSUE: 5/13/2009

QUESTION NO. : 19-333

In the response to RAI Question 19-43, a list of important "assumptions" made in the PRA regarding design features and operational requirements of the I&C systems (e.g., redundancy, separation, features to prevent spurious actuations, and testing and cooling requirements) is provided. However, this list does not appear to be adequately detailed and comprehensive. Please perform a systematic search to identify all important design and operational features of the I&C systems.

ANSWER:

Important "assumptions" made in the PRA regarding design features and operational requirements of the I&C systems are shown in table 1.

Table 1 Important assumptions

Assumptions		Disposition
General features of PSMS	Redundancy of four trains is provided.	DCD Section 7.2,7.3
	Redundant trains are appropriately separated.	DCD Section 7.1
	Digital part of I&C system is continuously checked by self-diagnosis function.	DCD Section 7.1
Features of RPS	Two RPS controllers per one train are diverse from each other, for reactor trip function.	DCD Section 7.2
	One channel of sensor is allowed to be unlimitedly bypassed.	DCD Chapter 16 Section 3.3
Features of EFAS and SLS.	ESFAS and SLS have parallel redundant controllers.	DCD Section 7.3
	One train of reactor trip breaker is allowed to be unlimitedly bypassed.	DCD Chapter 16 Section 3.3
	Reliability of PIF module is higher than front line components.	DCD Subsection 7.1.3.11
Feature of Non safety system	The non-safety GTG can be started manually when connecting to the class 1E bus in the event of station blackout.	DCD Section 8.4

Impact on DCD

No impact on DCD.

Impact on COLA

No impact on COLA.

Impact on PRA

No impact on PRA.