MITSUBISHI HEAVY INDUSTRIES, LTD.
1-1, WADASAKI-CHO, 1-CHOME, HYOGO-KU,
KOBE, 652-8585 JAPAN

April 9, 2014

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

Attention: Mr. Perry Buckberg

Docket No. 52-021
MHI Ref: UAP-HF-14036

Subject: MHI's Response to US-APWR DCD RAI No. 1091-7447 (SRP 07)

Reference: 1) "Request for Additional Information No. 1091-7447, SRP Section 07 – Instrumentation and Controls - Overview of Review Process - Application Section: 7," dated March 19, 2014.

With this letter, Mitsubishi Heavy Industries, Ltd. (MHI) transmits to the U.S. Nuclear Regulatory Commission (NRC) a document entitled "Response to US-APWR DCD RAI No. 1091-7447 (SRP 07)."

Enclosed are the responses to the questions contained within Reference 1.

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 of the RAI response (Enclosure 2), a copy of the non-proprietary version of the RAI response (Enclosure 3), and the Affidavit of Atsushi Kumaki (Enclosure 1) which identifies the reasons MHI respectfully requests that all material designated as proprietary in Enclosure 2 be withheld from disclosure pursuant to 10 C.F.R. § 2.390 (a)(4).

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 submittal. His contact information is provided below.

D081
NRO

Sincerely,

Atsushi Kumaki,
Manager, APWR Project Group
Global Nuclear Project Department
Nuclear Energy Systems Division
Energy & Environment Domain
Mitsubishi Heavy Industries, Ltd.

Enclosures:

1. Affidavit of Atsushi Kumaki

2. Response to US-APWR DCD RAI No. 1091-7447 (SRP 07) (Proprietary)

3. Response to US-APWR DCD RAI No. 1091-7447 (SRP 07) (Non-Proprietary)

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

ENCLOSURE 1

Docket No. 52-021
MHI Ref: UAP-HF-14036

MITSUBISHI HEAVY INDUSTRIES, LTD.
AFFIDAVIT

I, Atsushi Kumaki, being duly sworn according to law, depose and state as follows:

1. I am Manager, APWR Project Group, Global Nuclear Project Department, Nuclear Energy Systems Division, Energy & Environment Domain, 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 documents entitled "Response to US-APWR DCD RAI No. 1091-7447 (SRP 07)," dated April, 2014 and have determined that the document contains 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 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 the I&C design of the US-APWR.

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 and testing 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 the safety I&C system. Providing public access to such information permits competitors to duplicate or mimic the safety I&C system design without incurring the associated costs.

B. Loss of competitive advantage of the US-APWR created by benefits of enhanced plant safety, and reduced operation and maintenance costs associated with the safety I&C system.

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 9th day of April, 2014.

Atsushi Kumaki

Atsushi Kumaki,
Manager, APWR Project Group
Global Nuclear Project Department
Nuclear Energy Systems Division
Energy & Environment Domain
Mitsubishi Heavy Industries, Ltd.

Enclosure 3

Docket No. 52-021
UAP-HF-14036

Response to US-APWR DCD RAI No. 1091-7447 (SRP 07)

April 2014

(Non-Proprietary)

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

4/9/2014

US-APWR Design Certification

Mitsubishi Heavy Industries

Docket No.52-021

RAI NO.:	**NO. 1091-7447**
SRP SECTION:	**07 – Instrumentation and Controls**
APPLICATION SECTION:	**7**
DATE OF RAI ISSUE:	**3/19/2014**

QUESTION NO. : 07-1

Chapter 7 of the US-APWR DCD Revision 4 specifies that MHI has used the PRA results and insights in support of the US-APWR design. The staff acknowledges the MHI's intent in using the PRA to help improve the reactor design. However, in order to reach its safety conclusion on the Chapter 7 review and the acceptability of the reliability goals mentioned in Chapter 7, the staff needs additional information to understand the correlation between US-APWR DCD Chapter 7 and Chapter 19 information. Specifically:

1. Page 7.1-20, subsection 7.1.3.16, of the US-APWR DCD Revision 4 states that "As described in the probabilistic risk assessment (PRA) the RPS meets the plant reliability goals with only three channels in operation except the neutron flux monitoring function. Refer to the PRA Technical Report (Reference 7.1-16)." Please define the term "plant reliability goals" mentioned in the above statement, justify the acceptability of these goals, and explicitly identify the US-APWR PRA (Reference 7.1-16) section(s) which supports the use of only three channels in operation to meet those goals.
2. Page 7.5-7, subsection 7.5.1.1.4 (5), states that "The US-APWR PRA directly models instrument reliability using generic data, and the PRA is used to analyze the plant design to confirm that system reliability goals, such as those set for the maintenance rule, are acceptable. PAM instruments will be procured with sufficient reliability to be consistent with the generic reliability data used in the PRA, Chapter 7 of MUAP-07030." Please clearly define the term "system reliability goals," justify the acceptability of these goals, and describe the relationship with the maintenance rule. Describe how the PRA is used to confirm the system reliability goals.
3. Page 7.8-5, subsection 7.8.1.2.1, states that "The four pressurizer pressure signals are interfaced from each of the four PSMS trains. This configuration allows the DAS to meet the target reliability of the PRA with one channel continuously bypassed or inoperable." Please define the term "target reliability of the PRA," and clarify which section(s) of the PRA evaluates and discusses this issue.

ANSWER:

DCD Chapter 7 uses the PRA as a reference, not to establish design requirements. To clarify that intent, MHI will make those changes discussed below.

1. MHI's intent was for Subsection 7.1.3.16 to explain that the RPS, with exception of the neutron flux monitoring function, is conservatively modeled in the PRA with three channels operable in case one channel is failed. It was not MHI's intent to discuss the plant reliability goal in Chapter 7. This reference will be deleted because MHI recognizes this reference is not essential for the review of DCD Chapter 7.

2. Subsection 7.5.1.1.4(5) is to explain that procured PAM instruments will have reliabilities consistent with those values used for instrument generic data used in the PRA. The subsection will be revised to clearly state this.

3. US-APWR PRA assumes a failure probability of 1.0E-02 for the DAS, which is based on the DAS design for the DCD. The term "target reliability" in Subsection 7.8.1.2.1 is referring to this failure probability. The reference will be deleted because MHI recognizes this reference is not essential for the review of DCD Chapter 7.

Impact on DCD

DCD Subsections 7.1.3.16, 7.5.1.1.4, and 7.8.1.2.1 will be revised as shown in Attachment-1.

Impact on R-COLA

There is no impact on the R-COLA.

Impact on PRA

There is no impact on PRA.

Impact on Topical/Technical Report

There is no impact on Topical and Technical Reports.

7.1.3.15 Information Displays

Details on information displays are presented in Topical Report MUAP-07007, Chapter 18, and Section 7.5.

7.1.3.16 Consideration of Control System Induced Transients

Failures of the PCMS are bounded by the AOOs analyzed in the safety analysis, described in Chapter 15. These PCMS failures are described in Subsection 7.7.2.3. Chapter 8, Subsection 8.3.1.1.11 describes conformance to RG 1.204. This conformance bounds the envelope considered for PCMS EMI susceptibility. The PCMS uses the same hardware as the PSMS, which is qualified to RG 1.180. Therefore, additional lightening induced failures of the PCMS are precluded.

In some cases, it is advantageous to employ signals derived from instrumentation that are also used in the protection trains. This practice reduces the need for separate non-safety instrumentation, which would require additional penetrations into reactor pressure boundaries and introduce the need to additional maintenance in hazardous areas. For each parameter where instrumentation is shared, the PCMS receives four redundant signals from each train of the RPS. The signal selection algorithm (SSA), within the PCMS, receives input from all safety-related process trains but passes only the second highest operable process signal value to the control system's automation algorithms. The reactor control systems also have a modified SSA using an average calculation process. (This average calculation for select signals in the reactor control system is different from the description in MUAP-07004 Subsection 4.2.5.) The SSA excludes process inputs that are failed or taken out of service for maintenance or testing.

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 continuously tested as follows:

- The PCMS employs the same self-test features as the PSMS. These features are described in Subsection 4.1.5 of MUAP-07005.
- The basic software configuration and application software configuration, within the PCMS controller, is periodically confirmed by the same manually initiated method described in Subsection 4.1.4.1.c of MUAP-07005.

Since the SSA uses only digital values obtained from the PSMS via the unit bus, all functions of the SSA are completely covered by self-testing; no additional manual tests are required. The digital values obtained from the PSMS are confirmed during CHANNEL CALIBRATION for the safety-related sensors.

This SSA within the PCMS allows the RPS to have one instrument channel inoperable or bypassed at all times except the neutron flux monitoring function while still complying with General Design Criteria (GDC) 24 (Reference 7.1-14) and IEEE Std 603-1991 (Reference 7.1-15). ~~As described in the probabilistic risk assessment (PRA) the RPS meets the plant~~ MIC-04-07-00001 | DCD_07-1

~~reliability goals with only three channels in operation except the neutron flux monitoring function. Refer to the PRA Technical Report (Reference 7.1-16).~~ MIC-04-07-00001 DCD_07-1

The shared instrumentation signals are interfaced through fiber optic data networks. As such, an electrical fault in the PCMS cannot propagate to the protection channel. Refer to MUAP-07004 Subsection 4.2.5 for additional details.

7.1.3.17 Life Cycle Process

MHI applies ~~its MELCO's safety system~~ fully digital platform for the safety-related I&C system, MELTAC, to the PSMS of the US-APWR. ~~Full details of the life cycle process for the MELTAC safety platform basic software, including quality assurance (QA), management, development, installation, maintenance, training, operation, and the software safety plan are discussed in MUAP-07005 Section 6.0.~~ The life cycle process for the PSMS application software, including QA, management, development, installation, maintenance, training, operation, and the software safety plan are discussed in The US-APWR Software Program Manual (Reference 7.1-18), including BTP 7-14 (Reference 7.1-17) compliance. ~~The life cycle process for the MELTAC platform basic software is described in JEXU-1012-1132, The Basic Software Program Manual (Reference 7.1-35).~~ The US-APWR Software Program Manual (MUAP-07017) also controls the basic software life cycle process of the MELTAC Platform. DCD_07.01-45 DCD_07.01-45

7.1.3.18 Quality Assurance Program

The overall quality assurance program (QAP) for the US-APWR I&C systems is described in Chapter 17. ~~The specific QAP for the MELTAC platform is described in MUAP-07005 Section 6.0. These QAPs address all requirements of Title 10, Code of Federal Regulations (CFR), Part 50, Appendix B (Reference 7.1-19), and IEEE Std 7-4.3.2-2003 (Reference 7.1-20).~~ DCD_07.01-45

7.1.3.19 Identification

I&C equipment identification follows the guidance of RG 1.75, which endorses IEEE Std 384-1992 (Reference 7.1-22). The following color coding is provided on tags used for the identification of I&C system cabinets and for stand alone components, such as field instruments.

Identification shall not require frequent use of reference material.

- Train A: Red with white lettering
- Train B: Green with white lettering
- Train C: Blue with white lettering
- Train D: Yellow with black lettering
- Non-safety train: White with black lettering

This color coding is consistent with the color coding defined in Subsection 8.3.1.1.8 identification of class 1E electrical equipment and cables.

497-2002 (Reference 7.5-2). Trend information for these variables is displayed on the operational VDUs as described in Subsection 7.5.1.1.1 and Figures 7.5-1 and 7.5-2.

(3) Response Time

A PAM channel is designed to provide real time and timely information. PAM signals are transmitted from the sensors to the VDUs through a digital control system. The response time between detection and indication is approximately one to three seconds. The update frequency is less than one second. Thus, the PAM channel has sufficient capability to provide real time and timely information.

(4) Required Instrumentation Duration

The operating time for each variable required for DBA conditions is addressed in the development of the qualification program, per Section 3.11 and Technical Report MUAP-08015. The design basis accident analyses provide the basis for the required durations.

a. The duration for Type A variables is determined from required operator action by the accident analysis and emergency procedure which duration is less than four months. All Type A variables are also other type. Therefore, the duration for Type A variables is required to be four months consistent with the duration for other type.

b. The duration for Type B variables is at least the duration associated with the longest-duration design basis event for that variable; four months is required by the accident analyses and emergency procedure of the US-APWR.
c. The duration for Type C variables is at least 100 days for instrument channels monitoring the fission product barriers; four months is required by the accident analyses and emergency procedure of US-APWR.
d. The duration for Type D and E is four months as required by the accident analyses and emergency procedure.

A shorter duration may be acceptable if equipment replacement or repair can be accomplished within an acceptable out-of-service time, taking into consideration the location and accessibility of the equipment. When PAM instrumentation is located inside containment, is inaccessible, the required duration is four months.

(5) Reliability

DCD Subsection 19.1.4.1.1, "Description of the Level 1 PRA for Operations at Power," states that for each component type and failure mode, the failure rates are extracted from available generic data sources. This section also makes two key assumptions related to component reliability:

- US generic data are applied for component reliability data
- US generic data are applied to component unavailability due to test and unplanned maintenance

The US-APWR PRA directly models instrument reliability using generic data~~, and the PRA is used to analyze the plant design to confirm that system reliability goals, such as~~ DCD_07-1

~~those set for the maintenance rule, are acceptable~~. PAM instruments will be procured with sufficient reliability to be consistent with the generic reliability data used in the PRA, Chapter 7 of MUAP-07030. ~~Therefore, assuring that system reliability goals are met.~~ DCD_07-1

7.5.1.2 Bypassed and Inoperable Status Indication

The system level BISI is provided based on RG 1.47 (Reference 7.5-4). These indications are displayed as the spatially dedicated continuously visible (SDCV) information on the LDP in the MCR. These indications can be monitored on the operational VDU in the MCR. The system level BISI is discussed in detail in the HSI/HFE Topical Report (Reference 7.5-3) Section 4.9.

7.5.1.2.1 Design of Bypassed and Inoperable Status Indication

BISI functions are provided from the status of PCMS and PSMS systems. BISI is a non-safety function implemented within the PCMS. The interface of BISI data signals from safety to non-safety systems uses the Unit Bus and therefore meets DI&C-ISG-04 in the same manner as other safety-related to non-safety data communications. Independence and physical separation are provided between redundant safety-related systems and between the safety-related and non-safety systems.

The system level BISI is provided in the "OK monitor" area on the LDP for inoperable conditions that result in inoperability of any ESF or RT system function at the train level. The BISI is color-coded so that the indication for each function is lighted in yellow color when one train is bypassed, and lighted in red color when two or more trains are bypassed. When the system level BISI are displayed on the LDP, operators can drill down to specific inoperable information in the train level on the operational VDU in the MCR.

With regard to certain items performed at least once per fuel cycle (i.e., up to 24 months while RG 1.47 recommends "per one year"), the system level BISI is automatically initiated by a signal from the PSMS and is not removed by any method until the initiating signal is reset from the PSMS. In addition, to the automatic initiation conditions listed below, the operator can manually initiate the system level BISI from the operational VDU.

- Connecting PSMS controller to the maintenance network
- PSMS input bypass to accommodate input calibration and testing
- RPS bypass for shunt trip testing
- Component bypass from SLS (to perform component maintenance)
- Bypass or alignment of the components and equipment of the following fluid system in positions that would bypass the safety function (that are tested at least once per 24 months during plant operation)
  - ECCS
  - CS/RHR System

The numbers of channels required for each automatic actuation function are based on the following considerations:

- No single failure spuriously actuates the DAS.
- Bypass of a single channel does not cause the DAS automatic function to be inoperable, prevent decisions regarding credited manual actions or prevent monitoring critical safety functions.

The defeat switch can be manually actuated during plant heatup and cooldown conditions to prevent actuation of the DAS when it is not needed. This is an administratively controlled operating bypass.

The DAS functional logic diagram for automated actuation is included on Figure 7.2-2 sheet 14.

The DAACs are located in separate Class 1E Electrical Rooms. To cope with seismic events, the DAACs are qualified as Seismic Category II.

7.8.1.2.1 Reactor Trip, Turbine Trip and Main Feedwater Isolation

Reactor trip, turbine trip and MFW isolation are automatically actuated on the following signals:

- Low pressurizer pressure: 2-out-of-4 voting logic of the four pressurizer pressure low signals.
- High pressurizer pressure: 2-out-of-4 voting logic of the four pressurizer pressure high signals.
- Low SG water level: 2-out-of-4 voting logic of the one SG water level low signals from each SG.

The four pressurizer pressure signals are interfaced from each of the four PSMS trains. ~~This configuration allows the DAS to meet the target reliability of the PRA with one channel continuously bypassed or inoperable.~~ DCD_07-1 MIC-04-07-00001

To support the single failure criterion for all PSMS functions, there are four SG water level signals (one per each train A, B, C, and D) on each SG. However, for the DAS, which does not need to meet the single failure criterion, only one water level signal is required from each SG.

The reactor trip is actuated by tripping the non-safety CRDM motor-generator set. This actuation leads to de-energizing the power for the CRDM by a means that is diverse from the RTB to release the control rods for gravity insertion into the reactor core. Diversity from the PSMS is maintained from sensor-inputs to final actuators.

The Turbine Trip is actuated by opening the solenoid valves for turbine trip. Diversity from the RT function in the PSMS is maintained from sensor-input up to the power interface module.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

4/9/2014

US-APWR Design Certification

Mitsubishi Heavy Industries

Docket No.52-021

RAI NO.:	**NO. 1091-7447**
SRP SECTION:	**07 – Instrumentation and Controls**
APPLICATION SECTION:	**7**
DATE OF RAI ISSUE:	**3/19/2014**

QUESTION NO. : 07-2

The staff requests that MHI provide further clarification for the following PRA-related information referenced in the MHI Technical Report MUAP-07004-P(R8), "Safety I&C System Description and Design Process:"

1. Page 71, Section 5.1.10 first full bullet on the page, states that "...the reliability of the safety function is sufficient to achieve the plant level probabilistic risk assessment (PRA) goals for core damage frequency (CDF) and large early release frequency (LERF). Refer to MUAP-07030 Attachments 6A.12 and 6A.13." Please specifically identify which section(s) of the MUAP-07030 Attachments 6A.12 and 6A.13 evaluates and supports the above conclusion. Furthermore, describe how the "plant large early release frequency (LERF)" versus "large release frequency (LRF)" is used in support of the US-APWR DC application as mentioned in the statement.
2. Page 95, Appendix A, section A.4.9, states that "The reliability analysis methods for the PSMS are described in Section 6.5.2. This analysis ensures that the PSMS meets the reliability requirements assumed in the Probabilistic Risk Assessment (PRA)." Please explicitly identify and describe the "reliability requirements assumed in the PRA" mentioned in the above statement.

ANSWER:

1. MHI's intent was only to reference the PRA for the reader's information, not be the basis of any portion of the I&C design. The reference to the PRA will be deleted because MHI recognizes this reference is not essential for the Chapter 7 review. It is noted that LERF was an editorial error, and will be deleted as well.

2. This sentence generically refers to the PRA, which models the PSMS and achieves the plant reliability requirement in terms of CDF and LRF (i.e., the US-APWR probabilistic safety target defined in DCD Subsection 1.2.1.2.2.2). The sentence will be revised to delete

the term "reliability requirement" because the technical report is not focused on the plant reliability requirement.

Impact on DCD

There is no impact on the DCD.

Impact on R-COLA

There is no impact on the R-COLA.

Impact on PRA

There is no impact on PRA.

Impact on Topical/Technical Report

Technical Report MUAP-07004 Subsections 5.1.10 and A.4.9 will be revised as shown in Attachment-2.

DCD_07-2

5.1.11 Minimum Inventory of HSI

Class 1E HSI is provided by the safety VDUs for all safety-related indications and controls. Spatially Dedicated Continuously Visible (SDCV) displays are provided for all critical safety function parameters and for bypassed and inoperable conditions. This data is obtained from the PSMS and PCMS. SDCV HSIs are provided for manual initiation of reactor trip and ESFAS. Additional SDCV HSIs may be provided to ensure timely operator actions for specific plant events. The complete minimum inventory of SDCV HSI is described in the HSI system Topical Report, MUAP-07007. The complete minimum inventory of SDCV HSI is also described in DCD Chapter 18.

5.1.12 Computer Based Procedures

Computer based procedure allows operators to access relevant display formats which are hyper linked from the procedure and shown on the operational VDU. The operator is able to access and operate the required control switch quickly from the linked display formats on the operational VDU, if necessary.

each other and isolated from non-safety systems. Isolation ensures functional and communications independence and independence for fires and electrical faults. The design life of PSMS components is maximized when operated continuously in a controlled ventilation environment. The PSMS will operate reliably for extended periods with loss of ventilation.

A.4.9 Reliability

The reliability analysis methods for the PSMS are described in Section 6.5.2. ~~This analysis ensures that the PSMS meets the reliability requirements assumed in the Probabilistic Risk Assessment (PRA).~~ The PSMS is modeled in the Probabilistic Risk Assessment (PRA) in accordance with this reliability analysis method. The PSMS includes either N trains or N+1 trains, depending on the application. N is the number of trains needed to meet the single failure criterion and the number of trains needed to meet the single failure criterion. DCD_07-2

A.4.10 The Critical Points in Time or the Plant Conditions

The PSMS automatically initiates appropriate protective actions when a plant condition monitored by the system reaches a preset level. The critical points in time are determined by the PSMS response time modeled in the accident analysis. The PSMS is designed and tested to meet the response times assumed in the accident analysis.

The operator can reset the PSMS system level actuation signal using a minimum of two distinct and deliberate actions. There are no automatic resets of the system level actuation signals.

A.4.11 Equipment Protective Provisions

No credible single failure of an equipment protective device prevents the initiation or accomplishment of a safety function at the system level.

The PSMS continuously checks internal conditions such as power supply and digital component operability. Components are automatically shut down under component failure conditions that may lead to unpredictable system performance. These checks are conducted independently within each train of the PSMS; therefore, a spurious shutdown of PSMS equipment will only affect one train.

The equipment protective features are designed to place the safety systems in a safety state, or into a state that has been demonstrated to be acceptable, if the safety-related equipment fails or the equipment protective device operates. Each protection function has different characteristics and therefore different techniques are used to achieve a fail-safe design. Examples of protective features for selected functions include:

- Reactor trip circuits are designed to fail in the tripped state.
- Engineered safety features actuated components are designed to fail into a de-energized state or fail as-is. The de-energized state applies to failures that result in complete loss of