ArevaEPRDCPEm Resource

From: WILLIFORD Dennis (AREVA) [Dennis.Williford@areva.com]
Sent: Thursday, February 21, 2013 2:54 PM
To: Snyder, Amy
Cc: Canova, Michael; DELANO Karen (AREVA); LEIGHLITER John (AREVA); ROMINE Judy (AREVA); RYAN Tom (AREVA); WILLS Tiffany (AREVA)
Subject: Response to U.S. EPR Design Certification Application RAI No. 555 (6611), FSAR Ch. 7, Supplement 2
Attachments: RAI 555 Supplement 2 Response US EPR DC.pdf

Amy,

AREVA NP Inc. provided a schedule for a technically correct and complete response to Questions 07.01-54 and 07.01-55 and a preliminary schedule for Question 07.01-53 of RAI No. 555 on September 24, 2012. On November 13, 2012, AREVA NP Inc. sent Supplement 1 to provide a final schedule for a technically correct and complete response to Question 07.01-53.

The attached file, "RAI 555 Supplement 2 Response US EPR DC.pdf," provides a technically correct and complete response to 2 of the remaining 3 questions, as committed.

The following table indicates the respective pages in the response document, "RAI 555 Supplement 2 Response US EPR DC.pdf," that contain AREVA NP's response to the subject questions.

Question #	Start Page	End Page
RAI 555 — 07.01-54	2	15
RAI 555 — 07.01-55	16	20

The schedule for a technically correct and complete response to the remaining question remains unchanged as provided below.

Question #	Response Date
RAI 555 — 07.01-53	April 1, 2013

Sincerely,

Dennis Williford, P.E.
U.S. EPR Design Certification Licensing Manager
AREVA NP Inc.
7207 IBM Drive, Mail Code CLT 2B
Charlotte, NC 28262
Phone: 704-805-2223
Email: Dennis.Williford@areva.com

From: WILLIFORD Dennis (RS/NB)
Sent: Tuesday, November 13, 2012 3:54 PM
To: Amy.Snyder@nrc.gov
Cc: BENNETT Kathy (RS/NB); DELANO Karen (RS/NB); LEIGHLITER John (RS/NB); ROMINE Judy (RS/NB); RYAN Tom

(RS/NB); Michael.Canova@nrc.gov
Subject: Response to U.S. EPR Design Certification Application RAI No. 555 (6611), FSAR Ch. 7, Supplement 1

Amy,

AREVA NP Inc. provided a schedule for a technically correct and complete response to Questions 07.01-54 and 07.01-55 and a preliminary schedule for Question 07.01-53 of RAI No. 555 on September 24, 2012.

The schedule for a technically correct and complete response to Question 07.01-53 has been evaluated and finalized and is included below. The schedule for the technically correct and complete response to the other two questions remains unchanged as provided below.

Question #	Response Date
RAI 555 — 07.01-53	**April 1, 2013**
RAI 555 — 07.01-54	February 21, 2013
RAI 555 — 07.01-55	February 21, 2013

Sincerely,

Dennis Williford, P.E.
U.S. EPR Design Certification Licensing Manager
AREVA NP Inc.
7207 IBM Drive, Mail Code CLT 2B
Charlotte, NC 28262
Phone: 704-805-2223
Email: Dennis.Williford@areva.com

From: WILLIFORD Dennis (RS/NB)
Sent: Monday, September 24, 2012 2:52 PM
To: Getachew.Tesfaye@nrc.gov
Cc: BENNETT Kathy (RS/NB); DELANO Karen (RS/NB); LEIGHLITER John (RS/NB); ROMINE Judy (RS/NB); RYAN Tom (RS/NB)
Subject: Response to U.S. EPR Design Certification Application RAI No. 555 (6611), FSAR Ch. 7

Getachew,

Attached please find AREVA NP Inc.'s response to the subject request for additional information (RAI). The attached file, "RAI 555 Response US EPR DC.pdf," provides a schedule since a technically correct and complete response to the three questions cannot be provided at this time.

The following table indicates the respective pages in the response document, "RAI 553 Response US EPR DC.pdf," that contain AREVA NP's response to the subject questions.

Question #	Start Page	End Page
RAI 555 — 07.01-53	2	3
RAI 555 — 07.01-54	4	6
RAI 555 — 07.01-55	7	9

The schedule for technically correct and complete responses to Questions 07.01-54 and 07.01-55 is provided below. A preliminary schedule for the response to Question 07.01-53 is also provided below. The schedule for the response to Question 07.01-53 is being reevaluated and a new supplement with a revised schedule will be transmitted by November 15, 2012.

Question #	Response Date
RAI 555 — 07.01-53	**November 15, 2012**
RAI 555 — 07.01-54	**February 21, 2013**
RAI 555 — 07.01-55	**February 21, 2013**

Sincerely,

Dennis Williford, P.E.
U.S. EPR Design Certification Licensing Manager
AREVA NP Inc.
7207 IBM Drive, Mail Code CLT 2B
Charlotte, NC 28262
Phone: 704-805-2223
Email: Dennis.Williford@areva.com

From: Tesfaye, Getachew [mailto:Getachew.Tesfaye@nrc.gov]
Sent: Friday, August 24, 2012 3:01 PM
To: ZZ-DL-A-USEPR-DL
Cc: Morton, Wendell; Zhang, Deanna; Spaulding, Deirdre; Mott, Kenneth; Truong, Tung; Zhao, Jack; Mills, Daniel; Jackson, Terry; Canova, Michael; Segala, John; ArevaEPRDCPEm Resource
Subject: U.S. EPR Design Certification Application RAI No. 555 (6611), FSAR Ch. 7

Attached please find the subject request for additional information (RAI). A draft of the RAI was provided to you on August 15, 2012, and on August 24, 2012, you informed us that the RAI is clear and no further clarification is needed. As a result, no change is made to the draft RAI. The schedule we have established for review of your application assumes technically correct and complete responses within 30 days of receipt of RAIs. For any RAIs that cannot be answered within 30 days, it is expected that a date for receipt of this information will be provided to the staff within the 30 day period so that the staff can assess how this information will impact the published schedule.

Thanks,
Getachew Tesfaye
Sr. Project Manager
NRO/DNRL/LB1
(301) 415-3361

Hearing Identifier: AREVA_EPR_DC_RAIs
Email Number: 4226

Mail Envelope Properties (554210743EFE354B8D5741BEB695E6560CC7E7)

Subject: Response to U.S. EPR Design Certification Application RAI No. 555 (6611), FSAR Ch. 7, Supplement 2
Sent Date: 2/21/2013 2:54:28 PM
Received Date: 2/21/2013 2:54:48 PM
From: WILLIFORD Dennis (AREVA)

Created By: Dennis.Williford@areva.com

Recipients:
"Canova, Michael" <Michael.Canova@nrc.gov>
Tracking Status: None
"DELANO Karen (AREVA)" <Karen.Delano@areva.com>
Tracking Status: None
"LEIGHLITER John (AREVA)" <John.Leighliter@areva.com>
Tracking Status: None
"ROMINE Judy (AREVA)" <Judy.Romine@areva.com>
Tracking Status: None
"RYAN Tom (AREVA)" <Tom.Ryan@areva.com>
Tracking Status: None
"WILLS Tiffany (AREVA)" <Tiffany.Wills@areva.com>
Tracking Status: None
"Snyder, Amy" <Amy.Snyder@nrc.gov>
Tracking Status: None

Post Office: FUSLYNCMX03.fdom.ad.corp

Files	**Size**	**Date & Time**
MESSAGE	5768	2/21/2013 2:54:48 PM
RAI 555 Supplement 2 Response US EPR DC.pdf	871677	

Options
Priority: Standard
Return Notification: No
Reply Requested: No
Sensitivity: Normal
Expiration Date:
Recipients Received:

Response to

Request for Additional Information No.555, Supplement 2

8/24/2012

U. S. EPR Standard Design Certification
AREVA NP Inc.
Docket No. 52-020
Review Section: 07.01-A Appendix - Acceptance Criteria and Guidelines for Instrumentation and Control Systems Important to Safety
Application Section: 7.1

Question 07.01-54:

Open Item

Follow up to RAI 505, Question 07.01-46

The staff requests the applicant to provide an analysis of the priority logic scheme for the U.S. EPR instrumentation and control (I&C) systems in order to verify the absence of potential conflicts between various I&C systems such as PS, SICS, SAS, PAS, and DAS that have the capability to control safety-related plant equipment. The staff is interested in how the priority logic scheme in conjunction with the duration and timing of activation/de-activation signals from I&C systems (that in some cases operate independently) would not prevent the safety function from continuing to completion during various operating scenarios. This RAI was created as a follow-up question to new design information provide to the staff within the applicant's response to RAI 505, Question 07.01-46 as well as other new design information provided to the staff in Phase 4 of the U.S. EPR design certification review.

IEEE Std. 603, Clause 5.2, "Completion of Protective Action". Clause 5.2 states, in part, that the safety systems shall be designed so that, once initiated automatically or manually, the intended sequence of protective actions of the execute features shall continue until completion. Technical Report ANP-10310P, "Methodology for 100% Combinatorial Testing of the U.S. EPR Priority Module Technical Report" Revision 1, defines a latched actuation signal as a priority module input that functions as follows. Following an actuation input signal transition from a valid logic "1" to a valid logic "0", the logic "1" continues to be used in processing (i.e., it is latched). When a different (pre-designated) actuation input signal (e.g., an actuation signal in counter-direction) transitions from a valid logic "0" value to a valid logic "1", the latched value returns to a logic "0" for use in processing. Technical Report ANP-10310P also defines a non-latched actuation signal as a priority module input whose logic value present as a valid input is the value used in processing. Section 5.2 of Technical Report ANP-10309P, "U.S. EPR Protection System Technical Report", Revision 4, states that, "The ALU also contains the logic used to latch and either manually or automatically un-latch actuation outputs." Section 8.1, "ENGINEERED SAFETY FEATURES ACTUATION" of Technical Report ANP-10309P, states, in part, that one of the activities performed in the ALU layer is signal latching. This section goes on to state that, "the actuation signal is latched via set-reset function block in the ALU to confirm completion of the function." The following are observations regarding the two technical reports:

1. Technical Report ANP-10309P does not clearly define the terms "latch" and "unlatch" with regards to system. Specifically, this section does not state whether the ALU is the only device in the U.S. EPR design that has the capability to latch or unlatch an output signal. In other words it is not known whether SAS, DAS, PAS, or SICS can also latch or unlatch a signal at the PACS module. Also, the definition of latched and unlatched does not appear to take into account the safety classification of the signal's originating system. Therefore, it is unknown if a system such as PAS or DAS can unlatch or latch a signal from a safety-related system.

2. It is not clear how a latched actuation signal adequately confirms completion of the function, as opposed to using feedback or checkback signals from the PACS modules that would demonstrate component operation has been completed.

3. Section 8.1 of Technical Report ANP-10309P also does not provide details on how an ALU can “manually” unlatch a signal, nor does it state the conditions, reasoning, and criteria that would make it acceptable to automatically unlatch an actuation output.

4. From the definitions in Technical Report ANP-10310P of latched and unlatched signals, there’s no clear delineation of how signal priority can be achieved. In terms of latched signals, there does not seem to be a limitation placed on what I&C system can initiate a logic transition, or ‘unlatch’ an actuation signal. The only criteria necessary is that an actuation signal in a counter direction be present. Overall, it is not clear whether these definitions are generically applicable to all interfacing I&C systems.

5. It is not clear how the definitions in Technical Report ANP-10310P correspond to how these signals are used in PS operation in Technical Report ANP-10309P.

Additional examples that demonstrate the need to clarify the priority logic scheme include the following. Section 7.3.1.2.2 of U.S. EPR FSAR Tier 2, Section 7.3.1.2.2, Revision 3, “Emergency Feedwater System Actuation [EFW]”, states that, “When EFW actuation occurs due to LOOP and SIS actuation, the PS sends a pulse of limited duration to start the actuation. The duration of the pulse is long enough for the intended actions of the execute features to go to completion.” The description of this signal described for EFW completion of action in Section 7.3.1.2.2 does not appear to be consistent with how Technical Report ANP-10309P describes how a latched signal is used to determined completion of the function. Furthermore, the staff is not clear as to how the EFW system will respond if a non-PS I&C system sends a signal to start or stop outside the PS pulse of limited duration. In U.S. EPR FSAR, Tier 2, Section 7.1.1.6.5, “Priority”, the applicant provides an outline of how signals from various safety and non-safety related systems are prioritized at the PACS module. This section states, in part, that the U.S. EPR I&C design allows for multiple systems to send request to a given actuator, in case of competing signals. However, the staff requires more clarification on how the priority logic interprets non-competing signals from different I&C systems, both safety and non-safety related. For example, based on the OICS, the staff understands that, under normal operating conditions PAS automatic signals have higher priority at PACS modules than SICS manual signals. This section does not explicitly state that the PACS module maintains or somehow retains the priority of signals it receives. The section also does not state how the prioritization is performed nor does the section provide any detail on how latched, unlatched, delayed, limited duration, or any other types of signals are used at the PACS modules in order to ensure priority. In terms of signals that have an associated time delay or duration, this section does not state how safety functions that utilize those types of signals have ensured priority and do not lose priority if the signal expires. Finally, it is not clear how safety functions that require sequencing of actions could not be interrupted. For instance, if a loss-of-offsite power event requires load shedding and re-sequencing of loads to the safety-related electrical bus, could systems such as DAS and PAS potentially impact the sequencing of equipment since they operate independent of the PS?

The staff request the applicant to address the following items in order to clarify the prioritization scheme for the U.S. EPR:

a. Provide an analysis that demonstrates the capability of the prioritization scheme to adequately address potential operating scenarios for each safety-related plant component that can be operated by multiple I&C systems. Identify the priority scheme for each plant component and describe how the scheme can address potential operating scenarios such

as concurrent and conflicting signals, non-concurrent signals (signals received at different times), and signals received during a coordinated sequence of actions.

b. Clarify the definition of the terms “latched” and “unlatched” in the U.S. EPR Design. In addition:

   b-1. Identify what devices in each I&C system latches and unlatches signals to the PACS modules and describe the reason for the latching/unlatching and how this is performed.

   b-2. Clarify how the priority scheme of the PACS module prevents a system of lower priority from latching or latching a signal from a system of a higher priority. For example, based upon the current definitions of latched and unlatched signals in Technical Report ANP-10310P, how is the DAS prevented from latching or unlatching a signal from the PS for a given actuator?

   b-3. Based upon the above reference to Technical Report ANP-10309P, Section 8.1, clarify how a latched signal for the ESF function confirms a completion of protective function.

   b-4. Clarify how check-back signals, as documented in Technical Report ANP-10310P, Section 2.0, are utilized by each I&C safety system for which they apply to.

   b-5. Clarify how an ALU can “manually” unlatch a signal. Also provide the criteria for when an ALU would automatically latch or unlatch a signal.

c. Identify all safety functions that utilize pulse signals of limited duration. Provide a technical basis on why those functions use limited duration signals as opposed to a latched signal and justify why the use of limited duration signals is an acceptable means to verify completion of protective action.

d. Document all the specific system functions and applications for which delayed actuation signals are used. Provide a technical basis for why they are used in each instance. In addition:

   d-1. Are there differences in the amount of delay for various delayed actuation signals? If so, why and provide clarifying details.

   d-2. Is the PS, SAS, etc. responsible for attaching a time delay for these signals or are these signals all have a pre-defined time delay?

   d-3. How would a failure of this type of signal manifest itself? Provide details on how would its failure affect system functions or performance?

e. Is signal latching/unlatching for safety systems verified through periodic maintenance? If so, how is this done?

Response to Question 07.01-54:

1. The terms “latch” and “unlatch” are used to describe the use of the memory logic block (shown in U.S. EPR FSAR Tier 2, Figure 7.1-1). Latching a signal is referring to the input into the “set” portion of the memory logic block. Unlatching a signal is referring to the input into the “reset” portion of the memory logic block. The memory logic block is capable of being programmed into any function processor just the same as any other logic block shown U.S. EPR FSAR Tier 2, Figure 7.1-1. The PS, SAS, and DAS have the capability to latch and unlatch their own outputs to the PACS. For the SICS inputs to the PACS, the PACS has the capability to latch and unlatch its own outputs to the actuator. (Refer to the new U.S. EPR FSAR Tier 2, Figure 7.1-21 (Sheets 1 and 2)). Refer to the U.S. EPR FSAR Tier 2, Sections 7.2, 7.3, and 7.6, for the PS and SAS logic implementing the memory logic block to determine how a signal is latched or unlatched.

   The PACS priority module logic diagram will be included in U.S. EPR FSAR Tier 2, Section 7.1.

   The terms “latch” and “unlatch” will be clarified in ANP-10309P.

2. A latched signal from I&C systems such as PS, SAS, DAS, and PAS maintains a signal to the PACS to prevent any lower priority signal from interfering with a higher priority signal. For the SICS inputs to the PACS, the PACS has the ability to latch its outputs to the actuator so that the actuator goes to its end position and does not stop mid-travel. Once the actuator is in the desired end position, indication is provided in the main control room. The PACS removes its outputs to actuate and the higher priority signal is maintained to the PACS to prevent other systems from actuating the device in an undesirable position. This adequately confirms the completion of the function.

   For example, the PS closes the main steam isolation valves (MSIVs) and latches its signal to maintain the close signal. The PACS closes the MSIVs until the MSIVs are in the fully closed position. After the MSIVs are fully closed, the PACS removes its actuation outputs and does not provide any actuation signals to the actuators. As long as the PS maintains its close signal, open signals from any other system cannot open the main steam isolation valves. It is only when the accident conditions have cleared, and the MSIV closure signal is manually reset, that the other systems such as PAS or SICS may open the MSIV. Because of this, the MSIV stays closed as long as the accident conditions are present.

   If a feedback or checkback signal from PACS was used to reset the PS signal, then a non-safety system could come in after a device has reached its end position and actuate the device to an undesirable position. The PS does not receive feedback and checkback signals from the PACS to prevent other systems from placing the device into an undesirable position.

   U.S. EPR FSAR Tier 2, Section 7.1.3.6.13 will include additional detail on how latching adequately confirms the completion of a function.

3. For the U.S. EPR design, automatic safety-related actuation functions’ output signals must be reset manually by the operator from PICS or SICS unless there is justification for the functions’ signals being reset automatically.

The only ESFAS functions that are automatically reset are the PSRV Opening, CVCS Charging Isolation, EFW Actuation, and EFW Isolation. The PSRV Opening function signal is reset automatically because once the accident condition clears (Hot Leg Pressure goes below the protection high level setpoint) the PSRV automatically closes (spring loaded). The CVCS Charging Isolation function signal is reset automatically because the operator will reinitiate CVCS as soon as possible once the accident condition clears (PZR Level goes below the protection setpoint). The CVCS system is reinitiated manually by the operator once the accident condition clears. The EFW Actuation function's output signal is reset both manually (at any point in time) and automatically (when the accident condition clears, SG Level goes above the protection setpoint). The automatic reset of the EFW Actuation output signal is to provide priority to the SAS SG Level Control function once the SG Level goes above the protection setpoint. The EFW Isolation function's output signal is reset both manually (at any point in time) and automatically (by an EFW Actuation signal). The automatic reset of the EFW Isolation output signal is to provide EFW Actuation the priority to mitigate the low SG level event, if there is a low SG level event after a EFW Isolation has occurred.

The ESF Control and EAS functions are all automatically reset (unlatched) once the accident condition clears.

The output signals are not latched/unlatched because the following are control functions (using PI controllers) that require momentary signals to modulate a control valve to match the plant parameters:

- EFWS SG Level Control, EFWS Pump Flow Protection.
- MSRCV Control.
- SWCWS Condenser Supply Water Flow Control.
- CRACS Pressure Control, CRACS Cooler Temperature Control.
- SBVSE Supply Air Temperature Control for Supply Air Cooling.
- SIS/RHRS Automatic RHRS Flow Rate Control.

The output signals are automatically reset once the accident condition clears because the operator will reinitiate the equipment as soon as possible once the accident condition clears for the following functions:

- AVS Accident Filtration Train Heater Control.
- CCWS Emergency Temperature Control.
- FPCPS Pump Trip on Low SFP Level.
- CRACS Iodine Filtration Train Heater Control.
- CRACS Heater Control for Outside Inlet Air, SBVSE Supply Fan Safe Shut-Off.
- SBVSE Exhaust Fan Safe Shut-Off.
- SBVSE Battery Room Supply Air Temperature Control.
- CCWS Emergency Leak Detection-Switchover Valves Leakage or Failure.

The output signals are automatically reset because the function is designed to keep the plant within the safety setpoints (similar to the EFW Actuation and Isolation on SG Level). When the plant is within the safety setpoint limits, the priority will be given to the non-safety control functionality for the following functions:

- ESWPBVS ESWS Pump Rooms Temperature Control.
- FBVS Safety-Related Room Heater Control.
- FBVS EBS/FPCS Pump Rooms Heat Removal.
- SBVS SIS/RHRS Pump Rooms Heat Removal.
- SBVS CCWS/EFWS Valve Rooms Heat Removal.
- SBVSE Supply and Recirculation-Exhaust Air Flow Control.
- SBVSE Recirculation Fan Safe Shut-Off.
- SBVSE Supply Air Temperature Heater Control.
- SBVSE Freeze Protection, SBVSE Battery Room Heater Control.
- SBVSE EFWS Pump Room Heat Removal.
- SBVSE CCWS Pump Room Heat Removal.

The output signals are automatically reset because the design of switchover functions with latched output signals could provide situations of concurrent and conflicting actuation signals from the same function. Once the switchover function has executed, the lower priority commands will have control over the actuator (e.g., manual and non-safety) for the following functions:

- AVS Accident Train Switchover.
- CCWS Common 1.b Automatic Backup Switchover of Train 1 to Train 2 and Train 2 to 1.
- CCWS Emergency Leak Detection.

The output signals are automatically reset because the design of switchover functions with latched output signals could provide situations of concurrent and conflicting actuation signals from the same function. Once the switchover function has executed, the lower priority commands will have control over the actuator (e.g., manual and non-safety) for the following functions:

- CCWS Switchover Valve Interlock.
- CCWS RCP Thermal Barrier Containment Isolation Valve Interlock.
- SCWS Train 1 to Train 2 Switchover on Train 1 Low Evaporator Flow/Chiller Blackbox Internal Fault/SCWS Chiller Evaporator Water Flow Control/LOOP Re-Start Failure Interlock.
- SCWS Train 2 to Train 1 Switchover on Train 2 Low Evaporator Flow/Chiller Blackbox Internal Fault/Loss of UHS-CCWS/SCWS Chiller Evaporator Water Flow Control/LOOP Re-Start Failure Interlock.

- SCWS Train 3 to Train 4 Switchover on Train 3 Low Evaporator Flow/Chiller Blackbox Internal Fault/Loss of UHS-CCWS/SCWS Chiller Evaporator Water Flow Control/LOOP Re-Start Failure Interlock.
- SCWS Train 4 to Train 3 Switchover on Train 4 Low Evaporator Flow/Chiller Blackbox Internal Fault/SCWS Chiller Evaporator Water Flow Control/LOOP Re-Start Failure Interlock.
- CCWS RCP Thermal Barrier Containment Isolation Valves Opening Interlock functions,

For the In-containment Refueling Water Storage Tank System (IRWST) Boundary Isolation for Preserving IRWST Water Inventory Interlock function, the output signals are automatically reset once the accident condition clears because the valves are reinitiated by the operator as soon as possible once the accident condition clears.

The RHR Isolation Valves Interlock function prevents an unsafe valve configuration for the RHR system. For the RHR Isolation Valves Interlock function, the output signals are automatically reset once the valve positions are in a safe configuration because the operator will manually actuate these valves as soon as possible once the valves are in a safe configuration.

U.S. EPR FSAR Tier 2, Section 7.1 will be revised to include the design criteria for latching/unlatching and for manually or automatically unlatching a signal.

4. These definitions for latched and unlatched should not be applied generically to all interfacing I&C systems. The priority module logic diagram (U.S. EPR FSAR Tier 2, Figure 7.1-21 (Sheets 1 and 2)), shows which inputs are latched (through the use of the Memory logic block), nonlatched (no use of the Memory logic block), and delayed (through the use of Time Delay logic blocks). The priority module logic diagram (Figure 7.1-21 (Sheets 1 and 2)) shows how a signal may be unlatched in the PACS.

5. The EFWS actuation function is latched and unlatched both automatically and manually. The pulse duration is used to initiate the EFWS actuation on SIS and LOOP from the PS; then the signal is removed so the SAS EFWS SG level control function can have priority and control the EFWS level control valve.

The statement in the question: “under normal operating conditions PAS automatic signals have higher priority at PACS modules than SICS manual signals” is incorrect. The SICS always has higher priority than the PAS. U.S. EPR FSAR Tier 2, Section 7.1.1.6.5, states:

“The SICS manual component level commands are momentary signals that are latched in the PACS and unlatched once the actuator has reached its final limit position. Once the SICS component level command signal is unlatched in the PACS, the PAS has the ability to manipulate the actuator. This may be undesirable to the operator controlling the device.”

The priority module logic diagram (U.S. EPR FSAR Tier 2, Figure 7.1-21 (Sheets 1 and 2)), shows how latched inputs (through the use of the Memory logic block), nonlatched inputs (no use of the Memory logic block), and delayed inputs (through the use of Time Delay logic blocks) are used to provide logic for prioritization.

If a signal from PS, SAS, and PAS has a time duration, then once the signal expires the system does not have priority anymore in the PACS module. If a momentary signal from the SICS expires before the actuator reaches the final limit position, then the signal is latched in and PACS will continue to travel to the final limit position unless a higher priority signal is received or the final limit position is reached. Once the final limit position is reached, the PACS unlatches its signal and PAS has the ability to manipulate the actuator.

For the example of EDG loading sequence identified in the question, U.S. EPR FSAR Tier 2, Section 7.3.1.2.12, states:

> *"The PS performs the DLS functionality by maintaining an "off" signal to the actuators, and then removing the signal to a sub-set of actuators at each load step which allows them to be re-started. Essential service water (ESW) pumps and component cooling water (CCW) pumps are automatically started as part of the load sequence regardless of whether or not they were previously running."*

Other systems do not have the priority to interfere and overload the EDG. As shown in the priority module logic diagram (U.S. EPR FSAR Tier 2, Figure 7.1-21 (Sheets 1 and 2)), OFF has higher priority than ON; therefore, any signals from other systems to turn on these components will have lower priority than a PS OFF signal and will be ignored. The ESW and CCW pumps are started by the PS as part of the load sequence so that both systems' pumps are not turned on at the same time and potentially overload the EDG. Therefore, other systems cannot turn on both systems' pumps at the same time because the PS has the highest priority and already properly started them sequentially as part of the loading sequence.

Part a.

The priority scheme for every safety-related plant component is the same. U.S. EPR FSAR Tier 2, Section 7.1.1.6, lists the following systems inputs to the PACS in order of priority:

- PS/DAS.
- SAS.
- SICS.
- PAS.

Table 07.01-54-1 provides an analysis of this priority scheme when applied to various interfacing signal conditions:

Signals with overlapping durations (e.g., a safety-related pulse signal conflicting with a non-safety-related control signal of longer duration) and signals received during a coordinated sequence of actions can be treated as a combination of the concurrent and conflicting signals (for the time period that both signals are present) and non-concurrent signals (for the time period that only one of the conflicting signals is present). In both of these cases, the outcome is still the safety-related actions with the higher priority will maintain the plant in a safe state.

U.S. EPR FSAR Tier 2, Section 7.1.1.6.5, will be revised to include the description for the prioritization scheme analysis.

Part b.

1. See the Response to Parts 1, 2, and 3.

2. The only system signal that is latched in the PACS is the SICS manual commands. All other systems' signals to the PACS are latched within their respective systems, and are not latched within the PACS. The latching and unlatching of a signal is determined by how the Memory logic block is implemented in a system. See the logic diagrams for the respective systems to determine how the Memory logic block and latching/unlatching is implemented.

3. See the Response to Part 2.

4. Checkback signals are used in PACS to remove the PACS actuation output signal once the actuator has reached its final position. SICS and PAS use the checkback signals for indication and display in the MCR and RSS. The PS, SAS, and PAS uses checkback signals when device status or position is involved with the execution of a function (e.g., interlocks and SBVSE Supply and Recirculation-Exhaust Air Flow Control).

   U.S. EPR FSAR Tier 2, Figures 7.1-2, 7.1-6, and 7.1-8, will be revised to show a bi-directional hardwire signal between the PS and PACS.

5. An ALU can manually unlatch a signal when a Manual Interface logic block is connected to the reset side of a Memory logic block (e.g., U.S. EPR FSAR Tier 2, Figure 7.3-2–SIS Actuation). See the Response to Part 3 for the criteria when an ALU would automatically latch or unlatch a signal.

Part c.

The following safety-related functions use the Pulse Function logic block (shown in U.S. EPR FSAR Tier 2, Figure 7.1-1):

- EFWS Actuation on SIS and LOOP (U.S. EPR FSAR Tier 2, Figure 7.3-3): The Pulse Function logic block is used to maintain the actuation signal, until the actuator reaches its final position; then the actuation signal is removed, and the EFW SG Level control maintains the level. The safety protective function is completed once the EFW is initiated and the valves and pumps are in their final position or state.

- CVCS Charging Isolation (U.S. EPR FSAR Tier 2, Figure 7.3-21): The Pulse Function logic block provides a minimum actuation output time to maintain an actuation signal, until the actuators reach their final position. A pulse order is used to provide assurance that the actions of the execute features go to completion.

- CCW Emergency Temperature Control (U.S. EPR FSAR Tier 2, Figure 7.3-34): The Continuous Pulse Function logic block is used to close the heat exchanger bypass valve 10 percent of its 0-100 percent range at 1 minute intervals. This provides a gradual opening of the heat exchanger bypass valve and, therefore, a gradual cooling to the heat exchanger. The Continuous Pulse Function logic block is initiated by a high heat exchanger temperature, and is the continuous pulse is ended falls below the high setpoint or the heat exchanger bypass valve is in the fully closed position. This provides

assurance that the actuation signal is maintained until the execute features go to completion.

- SBVSE Supply and Recirculation-Exhaust Air Flow Control (U.S. EPR FSAR Tier 2, Figure 7.3-48): The Pulse Function logic block provides a minimum actuation output time to maintain an actuation signal, until the actuators reach their desired position. A pulse order is used to provide assurance that the actions of the execute features go to completion.

- SWCS Train Switchover Interlock Functions (U.S. EPR FSAR Tier 2, Figures 7.6-5 to 7.6-8): The Pulse Function logic block is used so that the circulating pumps are started and run to full speed, before the actuation signal is removed. A pulse order is used to provide assurance that the actions of the execute features go to completion.

- CCWS RCP Thermal Barrier Containment Isolation Valves Opening Interlock (U.S. EPR FSAR Tier 2, Figure 7.6-12): The Pulse Function logic block is used so that once an operating common header isolated, a momentary signal opens the standby common header and isolates the rest of the operating common header. This provides a momentary signal to switchover from an operating common header to the standby common header. The momentary signal's duration maintains an actuation signal, until the actuators reach their final position. A momentary signal is used to prevent concurrent and conflicting signals to the actuators between the CCW RCP Thermal Opening function, and the CCWS RCP Thermal Barrier Containment Isolation Vales Interlock for maintaining independence between the CCW trains feeding the RCP thermal barrier. A pulse order is used to provide assurance that a complete switchover between common headers occur.

U.S. EPR FSAR Tier 2, Sections 7.3 and 7.6, will be revised to include the description for the use of the Pulse Function logic block.

Part d.

The following safety-related functions use the On and Off Time Delay logic blocks (shown in U.S. EPR FSAR Tier 2, Figure 7.1-1):

- P7 Permissive Logic (U.S. EPR FSAR Tier 2, Figure 7.2-34): The Time Delay logic block is used in the P7 permissive function to consider the pump coast down time before validating the permissive and considering the RCPs totally off.

- MFWS SSS Isolation on SG Level > Max0p and RT Initiated for a Period of Time (U.S. EPR FSAR Tier 2, Figure 7.3-16): The Time Delay logic block is used in the MFWS SSS Isolation function to isolate all main feedwater (i.e., SSS Isolation) if a high SG level (SG level > Max0p) is present after a RT and MFW full load isolation (both on SG level > Max1p) has occurred. The time delay is used to provide a wait time after a RT and MFW full load isolation, for the SG level to decrease below the Max0p setpoint. If the after the time delay expires if the SG level is above the Max0p setpoint, it is necessary to isolate all main feedwater.

- EDG Actuation (U.S. EPR FSAR Tier 2, Figure 7.2-34): There are two types of uses for the Time Delay logic block for the EDG Actuation function. One for preventing spurious starts of the EDG on dips in the voltage. This is the time delay that is paired with each Threshold logic block on the EDG Actuation logic. The operator receives an alarm if the voltage degrades for longer than the first set of time delays. The second time delay in the downstream logic allows the operator time to correct the degraded voltage condition once he has received an alarm. If the operator does not correct the degraded voltage condition by the time period of the second time delay, then the EDG will be started and loaded so that the electrical bus is on a known good source.

- RCP Trip (U.S. EPR FSAR Tier 2, Figure 7.3-27): The Time Delay logic block is used in the RCP Trip function to delay the opening of the RCP bus supply circuit breaker so that simultaneously opening of RCP circuit breakers does not cause an excessive voltage surge.

- 7.3-29 Turbine Trip: The Time Delay logic block is used for a loss of flow event (loss of one RCP) at 100 percent power that results in a Reactor Trip on Low-Low RCS Flow Rate (U.S. EPR FSAR Tier 2, Figure 7.2-11). The safety analysis assumes that at turbine trip LOOP occurs and results in the loss of the three remaining operating RCPs. The time delay duration is the minimum time to delay the loss of the remaining three RCPs, to allow the trip to reduced power sufficiently, such that the loss of the remaining three RCPs does not challenge DNB limits.

- SWCS Train Switchover Interlock Functions (U.S. EPR FSAR Tier 2, Figures 7.6-5 to 7.6-8): The Time Delay logic block is used to start the pumps in a sequenced fashion (one pump at a time) and so that they are running full speed before they are loaded to the system.

U.S. EPR FSAR Tier 2, Chapter 7, Section 7.3, will be revised to include the description for the use of the On and Off Time Delay logic blocks.

1. There are differences in the amount of time delay for the instances where the Time Delay logic block is used. The delay times are specific for each function, dependent upon the accident the function is mitigating and equipment behavior. For example: The time delay used in the P7 permissive function is used to consider the pump coast down time before validating the permissive and considering the RCPs totally off. The time delay needed for the RCP Trip function is to prevent an excessive voltage surge. Therefore, the time delays should not be equal for both functions because the time delay serves two different purposes.

2. The time delays are not assigned by the I&C system automatically. The time delays are configured when they are programmed into the application software.

3. The failure of the time delay software logic block would be detected by the continuous self-test and flagged as an error. The undetected failure of a single time delay software block would either actuate a component too early or too late. This is covered by the PS and SAS FMEA under the conditions of a undetected spurious or undetected blocking failure. The failure of multiple time delay software logic blocks would be considered a latent defect in the software and is considered a software common cause failure. This

failure is addressed in the U.S. EPR Diversity and Defense-in-Depth Assessment Technical Report (ANP-10304).

Part e.

Signal latching/unlatching in the PS and SAS is done in the software logic of the system. This is verified through the continuous self-test features and also through the periodic extended self-test. The PACS latching/unlatching is part of the priority logic, and the priority logic is verified through the ADOT periodic test.

Table 07.01-54-1: Prioritization Scheme Analysis

Signal Types	Effect on PACS	Effect on Plant
Concurrent and Conflicting	The PACS module provides the actuation for the actuation signal with the highest priority. For concurrent and conflicting SICS commands (SICS open and close), the PACS module will not provide any actuation outputs. For other systems' commands, the PACS module will be configured to either an OPEN/ON priority or CLOSE/OFF priority depending on the actuator.	The actions of the system with the highest priority are executed. Priority is defined such that safety-related actions have higher priority than non-safety; therefore, the plant will continue to operate in a safe manner.
Non-concurrent	For PS and SAS signals: The PACS module provides the actuation for the actuation signal present at that moment in time. Once the actuation signal is removed, the PACS removes its actuation signal to the actuator. For SICS signals: The PACS module provides the actuation for the SICS actuation signal. The PACS latches its output to provide an actuation signal until the device reaches its final limit position. Once the device reaches its final limit position, the PACS unlatches its output and does not provide an actuation signal. During this time period when the PACS module output is latched, if the SICS actuation signal is removed, the PACS module will continue provide an actuation signal until the device reaches its final limit position. During this time period when the PACS module output is latched and the SICS actuation signal is removed, if the PACS receives a conflicting SICS actuation signal, then the PACS module will stop its previous actuation and provide actuation signal for the new SICS actuation signal.	The actions of the system providing the actuation signal present at that moment in time are executed. If this action brings the plant to a unsafe state, then once the plant reaches a protection setpoint, the higher priority safety system shall provide an concurrent signal to maintain the plant in a safe state.

Signal Types	Effect on PACS	Effect on Plant
Combination of Both Concurrent and Non-concurrent (e.g., Overlapping signals for a period of time)	For the time period where the signals are concurrent, the PACS module behaves as described in the concurrent and conflicting signals section. For the time period where the signals are non-concurrent, the PACS module behaves as described in the non-concurrent signal section.	For the time period where the signals are concurrent and conflicting: The actions of the system with the highest priority are executed. Priority is defined such that safety-related actions have higher priority than non-safety, therefore the plant will continue to operate in a safe manner. For the time period where the signals are non-concurrent: The actions of the system providing the actuation signal present at that moment in time are executed. If this action brings the plant to a unsafe state, then once the plant reaches a protection setpoint, the higher priority safety system shall provide a concurrent signal to maintain the plant in a safe state.

FSAR Impact:

U.S. EPR FSAR Tier 2, Sections 7.1, 7.2, and 7.6, will be revised as described in the response and indicated on the enclosed markup.

Technical Report Impact:

Technical Report ANP-10309 will be revised as described in the response and indicated on the enclosed markup.

Question 07.01-55:

Open Item

Follow up to RAI 505, Question 07.01-46

The staff requests the applicant provide additional design information on the Operational I&C Disable Switches (OICS) including: (1) Identification of all operational situations for which the OICS would be used; (2) Clarification of the operational effects of the OICS on all affected I&C systems; and (3) Identification of the consequences of OICS to provide its safety function, including the impact on the plant and the ability of operators to fulfill credited actions and/or mitigate anticipated operational occurrences and postulated accidents. This RAI is a follow-on to RAI 505, 07.01-46.

IEEE Std. 603-1991, Clause 5.2, states in part, that the safety systems shall be designed so that, once initiated automatically or manually, the intended sequence of protective actions of the execute features shall continue until completion. Clause 6.2.1 states, in part, that means shall be provided in the control room to implement manual initiation at the division level of the automatically initiated protective actions. The means provided shall minimize the number of discrete operator manipulations and shall depend on the operation of a minimum of equipment. The applicant introduced the OICS in Revision 3 of the U.S. EPR FSAR, Section 7.1.1.6.5. The staff, upon reviewing the new design information, issued RAI 505, Question 07.01-46 to request clarification on the design functionality, implementation and other general questions. The applicant's response to RAI 505, 07.01-46 (Supplement 18) did not adequately address all of the staff's concerns regarding this newly submitted design attribute.

According to U.S. EPR FSAR, Tier 2, Section 7.1.1.6.5, Revision 3, the applicant states the following regarding OICS:

"During normal operation, the operational I&C disable switch on the SICS is set so that the PAS can send commands to the PACS. In this configuration, automatic commands from the PAS override manual commands from the SICS because of the nature of the manual control logic in the PACS. If the operational I&C disable switch is set to DISABLE by the operator, the PAS input will be disabled (i.e., the input signals from the PAS to the communications module will be blocked from being sent to the priority module), providing the priority of the SICS manual commands. The operational I&C disable switch disables PAS inputs, all other PACS inputs remain operational."

The applicant's revised interim Revision 4 FSAR section markup, submitted as part of its response to RAI 505, Question 07.01-46, states,

"The SICS manual component level commands are momentary signals that are removed once the actuator has reached its final limit position. Once the SICS component level command signal is removed, the PAS has the ability to manipulate the actuator. This may be undesirable to the operator controlling the device. Therefore, four safety-related Operational I&C Disable switches are implemented to prevent PAS from manipulating the actuator. During normal operation, the Operational I&C Disable switches on the SICS are set so that the PAS can send commands to the PACS. If at least two of the four switches (2 out of 4 voting) are set to DISABLE by the operator, the PAS input is blocked by the PAC modules. This blocking function

is implemented within the PACS. The Operational I&C Disable switches block PAS inputs. The other PACS inputs remain operational."

In Revision 3 of FSAR Section 7.1.1.6.5, the applicant states that the automatic Process Automation System (PAS) commands normally override any SICS commands because of the nature of manual control logic at the Priority and Actuator Control System (PACS). This appears to be a design inconsistency in terms of the priority logic at the PACS module if a non-safety related system can override the commands of any safety-related I&C system (unless state-based priority logic is employed). In addition, when the OICS are enabled, the applicant states that PAS input will be disabled or blocked. The addition of the OICS is an indication that the applicant considers a failure of the non-safety related PAS to potentially impact safety functions. The staff could not determine, through a review of available documentation how the applicant addressed ta failure of the OICS.

The staff requests the applicant address the following questions:

a. Identify all operational situations for which the OICS would be used, including failures of PAS, AOOs, PAs, etc. Also clarify whether the SICS is, under normal conditions, at a higher priority than the PAS.

b. Identify the consequences of failure of OICS to provide their safety function on the plant and the ability of operators to fulfill credited actions and/or mitigate anticipated operational occurrences (AOOs) and postulated accidents (PAs).

c. Is the functionality provided by the OICS, considering it is safety-related, documented in Chapter 15? Per the definition of a safety function in IEEE Std. 603-1991, it appears the OICS functionality would be essential to help maintain plant parameters within acceptable limits established for a design basis event.

d. The applicant states, in part, that enabling 2oo4 OICS will, "….block PAS inputs, all other PACS inputs remain operational":

   d-1. Does this mean that all PAS inputs to all PACS communication modules will be blocked? If so, how does this affect the overall operations of PAS and other systems that are affected by PAS functionality?

   d-2. Does enabling the switches cause a complete loss of manual component or manual grouped control functionality on PICS?

   d-3. Does the PACS perform the blocking of PAS inputs? If so, describe in details how this blocking takes place on the PACS when a 2oo4 vote is received.

   d-4. In terms of the 2oo4 voting logic in the OICS: (i) Does this take place within the PS? (ii) Is this hardwired logic? (iii) Does the applicant have a figure that demonstrates this voting configuration for the staff's review?

e. Is OICS functionality required at the RSS? If not, provides details on why its functionality is not necessary at the RSS.

f. U.S. EPR FSAR markup, Page 7.1-51, states "The SICS manual component level commands are momentary signals that are removed once the actuators has reached its final limit position." Explain why the SICS manual controls are momentary signals and why the priority logic is not (or cannot be) implemented in a way that ensures SICS commands always have priority over PAS in all operational situations for a given actuator.

g. Is OICS functionality verified through periodic surveillance testing?

Response to Question 07.01-55:

Part a.

During normal operation, the PICS will be used for manual component level commands and the SICS manual component level commands are not the preferred method. For AOOs and PAS, where the SICS manual component level commands are the credited means for mitigating the event, it may be necessary that the OPDIS switch is used to prevent interference from the PAS (e.g., isolating the failed line for failures of small lines carrying primary coolant outside the reactor building),. The situations where the OPDIS switch would be used are described in the plant procedures and in U.S. EPR FSAR Tier 2, Section 7.1.

The SICS always has higher priority than the PAS. U.S. EPR FSAR Tier 2, Section 7.1.1.6.5 states:

> *"The SICS manual component level commands are momentary signals that are latched in the PACS and unlatched once the actuator has reached its final limit position. Once the SICS component level command signal is unlatched in the PACS, the PAS has the ability to manipulate the actuator. This may be undesirable to the operator controlling the device."*

Part b.

If the OPDIS switches are unable to perform their safety function, then the non-safety PAS may be able to change the final position of an actuator upon completion of the pulse signals from SICS when the operator is using the credited SICS manual component level commands. However, the OPDIS switches are hardwired and configured in a 2-out-of-4 fashion; therefore, the OPDIS switches will continue to provide their safety function considering a single failure.

Part c.

U.S. EPR FSAR Tier 2, Chapter 15 Safety Analysis, does not go into the level of detail describing the exact actions the operator will provide (e.g., component level commands versus grouped commands). It just describes the functions credited to the operator. The plant procedures and U.S. EPR FSAR Tier 2, Section 7.1, provide the details of how the operator may execute certain functions. The OPDIS switches are safety-related, and their use with the SICS manual component level control will be clarified in the U.S. EPR FSAR Tier 2, Section 7.1.

Part d.

1. "Block PAS inputs, all other PACS inputs remain operational" means that all of the control signals from the PAS communication module will be blocked by the PACS priority module. See the logic diagram for the PACS priority module (U.S. EPR FSAR Tier 2, Figure 7.1-21 (Sheets 1 and 2)) to see the OPDIS input interface. All actuation signals from the PAS are blocked by the PACS modules. Therefore, the manual commands from PICS to safety-related components are also blocked. All other functionalities of

PAS operate properly. This includes the control of non-safety-related equipment receiving checkback signals from the PACS and sending information to PICS for display.

2. Enabling the switch does not cause a complete loss of PICS manual command capabilities. Once the switch is enabled, the PICS manual commands to safety-related components are blocked because these manual commands are routed via PAS. PICS manual commands to non-safety components continue to operate properly.

3. Blocking of the PAS commands is done by the PACS module. Once the OPDIS switches provide 2-out-of-4 vote signal, this is sent to the priority module of the PACS. The priority module of the PACS, upon receiving the OPDIS signal, blocks the actuation inputs from the communication module. This prevents the PAS from actuating a safety-related component. See the logic diagram for the PACS priority module (U.S. EPR FSAR Tier 2, Figure 7.1-21 (Sheets 1 and 2)) to see the OPDIS input interface.

4. The 2-out-of-4 voting of the OPDIS switches is implemented in hardwired logic in the SICS. A diagram showing the 2-out-of-4 configuration will be included in U.S. EPR FSAR Tier 2, Section 7.1.

Part e.

The OPDIS is not necessary in the RSS. In the RSS the PICS and PAS provide the majority of the functionality necessary to bring the plant to a safe shutdown. The use of the OPDIS switch would remove the PICS and PAS control functionality in the RSS, necessary to bring the plant to a safe shutdown.

There is only a small amount of SICS commands in the RSS, which are for functionality not implemented in PICS. These SICS commands are system-level, routed via the PS, and latched in. The SICS system-level manual commands are not susceptible to any PAS interference.

Part f.

The SICS manual component level commands are implemented in momentary signals, and are latched in until the actuator reaches its final position. This gives the operator the ability to actuate the device to its end position or a position in between. If the actuated device is a control valve, it is necessary to have a momentary signal to jog the valve in a mid-travel position. The SICS has priority over the PAS because of the priority logic. The logic for the priority (shown in the priority module logic diagram (U.S. EPR FSAR Tier 2, Figure 7.1-21 (Sheets 1 and 2)) is implemented in a way that the higher priority systems only block or override lower priority signals when they provide an actuate command. If no higher priority system provides an actuate command, then the lowest priority system shall have the priority.

Part g.

The OPDIS switch is verified periodically (every 24 months) as part of the Actuating Device Operational Test (ADOT). Technical Report ANP-10315 will be revised to include the OPDIS switches as part of the ADOT. U.S. EPR FSAR Tier 2, Chapter 16.0, Table 3.3.1-1, already includes the OPDIS switches.

FSAR Impact:

U.S. EPR FSAR Tier 2, Section 7.1, and Chapter 16, will be revised as described in the response and indicated on the enclosed markup.

Technical Report Impact:

Technical Report ANP-10315 will be revised as described in the response and indicated on the enclosed markup

U.S. EPR
Final Safety Analysis Report

MARKUPS

Interfaces

Table 7.1-4 shows the interfaces of the PACS.

Architecture

Figure 7.1-8—Priority and Actuator Control System Architecture provides a functional representation of the PACS.

The PACS is organized into four independent divisions located in the following buildings:

- Safeguard Buildings.
- Emergency Power Generating Buildings.
- Essential Service Water Pump Buildings.

In each division, there are safety-related and non-safety-related PACS equipment to interface with safety-related and non-safety-related actuators, respectively. The safety-related PACS and non-safety-related PACS equipment is located in separate cabinets.

The PACS is composed of priority modules and communication modules. One priority module and one communication module are provided for each actuator/black box.

The PACS receives actuation orders sent by the various DCS systems for prioritization. Signals are sent either via hardwired connections or a dedicated data connection to the PAS. Interfaces with actuation devices and actuated equipment (e.g., switchgear, torque and limit switches) are via hardwired connections. Checkback signals are used in PACS to remove the PACS actuation output signal once the actuator has reached its final position. SICS and PAS use the checkback signals for indication and display in the MCR and RSS. The PS, SAS, and PAS use checkback signals when device status or position is involved with the execution of a function. Priority between actuation requests from the various DCS systems is established by wiring the inputs using the priority principles described in Section 7.1.1.6.5. The PACS priority logic diagram is shown in Figure 7.1-21—PACS Priority Module Logic Diagram.

07.01-54

Equipment

The PACS is implemented primarily with subracks, priority modules, communication modules, and qualified isolation devices as needed. Fiber optic cable is used for the data connection between the PAS and the PACS.

The PACS equipment may be modified and upgraded as needed, but shall exhibit these characteristics.

Data connections exist between the PAS and PACS. However, this connection is only between the PAS and non-safety-related PACS communication module. Connections between the communication module and safety-related priority module are hardwired. The communication module is qualified as an associated circuit.

The safety-related I&C systems are implemented in four independent divisions. The safety-related I&C systems retain their ability to perform their function given a single failure of a common element to both the safety-related and non-safety-related systems concurrent with another single failure. The control systems implement signal selection algorithms and redundancy to minimize the possibility of a single failure that results in a DBE that also reduces the redundancy of the safety-related systems. The safety-related systems implement error detection algorithms to detect and accommodate failures.

7.1.1.6.5 Priority

The U.S. EPR I&C design allows for multiple I&C systems to send requests to a given actuator. To make certain that each individual actuator executes the proper action for the given plant condition, priority management rules for the PACS are provided. The following systems inputs to the PACS are listed in order of priority:

- PS/DAS.
- SAS.
- SICS.
- PAS.

07.01-54

The DAS is given a higher priority than the SAS because it is a functional substitute to the PS and is needed at this level of priority to verify proper operation of SAS functions on a SWCCF of the PS. The PACS priority logic diagram is shown in Figure 7.1-21—PACS Priority Module Logic Diagram.

The SICS manual component level commands are momentary signals that are removed once the actuator has reached its final limit position. Once the SICS component level command signal is removed, the PAS has the ability to manipulate the actuator. This may be undesirable to the operator controlling the device. Therefore, four safety-related Operational I&C Disable switches are implemented to prevent PAS from manipulating the actuator.

07.01-55

The Operational I&C Disable switch will be necessary for an AOO or PA for which the operator uses credited SICS component-level commands to mitigate the event. Once the component-level command from SICS has been completed, the opportunity exists for PAS to send a conflicting signal to the actuator. In this case, the Operational I&C Disable switch prevents the PAS command from interfering with the credited

component-level commands on SICS.

There are situations when SICS commands do not necessitate the use of the Operational I&C Disable switch. One example is the use of system-level manual commands on SICS. Credited system-level manual commands on SICS are latched in by either the PS or DAS to the PACS. Because these signals are unlatched by manual resets, PAS commands are not able to interfere and the Operational I&C Disable switch is not needed. Another example is the execution of surveillance testing of component-level SICS commands.

07.01-55

During testing, PAS control of a safety-related device is overridden by the component-level SICS commands, actuating the component to the test state (e.g., OPEN/CLOSE or ON/OFF). Once the test state is reached, the surveillance test ends and the SICS commands are removed. Control of the component is returned to PAS. The use of the Operational I&C Disable switch during a surveillance test prevents PAS from controlling safety-related components, even those outside of the scope of the surveillance test.

During normal operation, the Operational I&C Disable switches on the SICS are set so that the PAS can send commands to the PACS. If at least two of the four switches (2 out of 4 voting) are set to DISABLE by the operator, the PAS input is blocked by the PAC modules. This configuration is shown in Figure 7.1-30—Operational I&C Disable Switch Configuration. ~~This~~The hardwired logic is implemented within the SICS and the blocking function is implemented within the PACS. The Operational I&C Disable switches block PAS inputs. The other PACS inputs remain operational. This includes the control of non-safety related equipment, receiving checkback signals from the PACS, and sending information to PICS for display. Table 7.1-9—Prioritization Scheme Analysis provides an analysis of the priority scheme when applied to various interfacing signal conditions.

07.01-54

Signals with overlapping durations (e.g., a safety related pulse signal conflicting with a non-safety related control signal of longer duration) and signals received during a coordinated sequence of actions, can be treated as a combination of the concurrent and conflicting signals (for the time period both signals are present) and non-concurrent signals (for the time period that only one of the conflicting signals is present). In both of these cases, the outcome is still the safety related actions with higher priority will maintain the plant in a safe state.

7.1.2 Response Time

Figure 7.1-28—Definition and Allocation of Response Times shows the equipment and response times for the U.S. EPR design. The equipment shown in Figure 7.1-28 is defined as follows:

An FMEA for the protective functions executed by the PS is described in ANP-10309P (Reference 6). An FMEA for the functions executed by SAS is provided in Table 7.1-7. Demonstration of the single failure criterion for the execute features is provided with the description of the process systems in Chapter 5, Chapter 6, Chapter 8, Chapter 9, Chapter 10, and Chapter 11.

7.1.3.6.13 Completion of Protective Action (Clauses 5.2 and 7.3)

The safety-related systems meet the requirements of Clause 5.2 of IEEE Std 603-1998 (Reference 1). When initiated by a safety-related system, protective actions proceed to completion. Return to normal operation requires deliberate operator intervention.

Once opened by the PS, the reactor trip breakers remain open until the reactor trip signal has cleared and they are able to be manually closed. The reactor trip signal ~~is~~ can only be only cleared when the initiating plant variable returns to within an acceptable range.

07.01-54

A latched signal from I&C systems (e.g., PS, SAS, DAS, PAS) maintains a signal to the PACS to prevent any lower priority signal from interfering with a higher priority signal. For the SICS inputs to the PACS, the PACS has the ability to latch its outputs to the actuator so that it goes to its end position and doesn't stop mid-travel. Once the actuator is to the desired end position, indication is provided to the main control room, the PACS removes its outputs to actuate, and the higher priority signal is maintained to the PACS to prevent other systems from actuating the device to an undesirable position. This adequately confirms the completion of the function.

Refer to Section 7.3.2.3 for a description of completion of protection action for ESF actuation functions.

The execute features within the U.S. EPR are designed so that once initiated, the protective actions continue until completion, in accordance with IEEE Std 603-1998, Clause 7.3.

7.1.3.6.14 Quality (Clause 5.3)

The safety-related systems meet the requirements of Clause 5.3 of IEEE Std 603-1998 (Reference 1). The safety-related systems are within the scope of the U.S. EPR quality assurance program (QAP) described in Section 17.5. The TXS hardware quality is described in EMF-2110(NP)(A) (Reference 3).

The digital safety systems meet the additional guidance of IEEE Std 7-4.3.2-2003 (Reference 18). This guidance addresses software quality processes for the use of digital technology in safety systems.

Table 7.1-4—DCS Interface Matrix
Sheet 2 of 4

From	To	Type	Basis
DAS	SICS	Hardwired	Provide information to SICS regarding DAS operation (e.g., DAS reactor trip initiated)
	PAS	Hardwired	Provide DAS information to PAS for display on PICS, provide signals to PAS to coordinate logic on diverse reactor trip or ESF actuation
	RTB	Hardwired	Diverse reactor trip signal
	CRDCS	Hardwired	Diverse reactor trip signal
	TG I&C	Hardwired	Diverse turbine trip signal
	PACS	Hardwired	Diverse ESF actuation signals
PS	SICS	Hardwired	Provide information to SICS regarding PS operation (e.g., PS reactor trip initiated)
	SICS	Data	Provide information to QDS for graphical display and trends
	PICS	Data	Provide information to PICS regarding PS operation (e.g., PS reactor trip initiated)
	SAS	Hardwired	Initiate ESF controls following ESF actuation
	PAS	Hardwired	Provide signals to PAS to coordinate logic on reactor trip or ESF actuation
	RTB	Hardwired	Reactor trip signal
	CRDCS	Hardwired	Reactor trip signal
	TG I&C	Hardwired	Turbine trip signal
	PACS	Hardwired	ESF actuation and interlock signals
SAS	SICS	Hardwired	Provide information to SICS regarding SAS operation (e.g., PS reactor trip initiated)
	PICS	Data	Provide information to PICS regarding SAS operation (e.g., PS reactor trip initiated)
	PAS	Hardwired	Provide for coordination of logic between SAS and PAS (if needed)
	PACS	Hardwired	Safety control signals

07.01-54

Table 7.1-4—DCS Interface Matrix
Sheet 3 of 4

From	To	Type	Basis
RCSL	PICS	Data	Provide information to PICS regarding RCSL operation (e.g., ACT control mode)
	PAS	Hardwired	Provide command signals for actuators used in RCSL functions other than control rods (e.g., RBMWS components for Boron control)
	CRDCS	Hardwired	Actuation commands for control rods
	TG I&C	Hardwired	Turbine actuation signals related to reactivity control and limitation functions
PAS	PICS	Data	Provide process and safety indications to PICS, provide information to PICS regarding PAS operation (e.g., auto/manual status, etc)
	PACS	Data	Actuator commands
	Actuators/ Black Boxes	Hardwired	Actuator commands
	TG I&C	Hardwired	TG I&C actuation commands
SCDS	SICS	Hardwired	Distribute DCS input signals to SICS
	DAS	Hardwired	Distribute DCS input signals to DAS
	PS	Hardwired	Distribute DCS input signals to PS
	SAS	Hardwired	Distribute DCS input signals to SAS 07.01-54
	RCSL	Hardwired	Distribute DCS input signals to RCSL
	PAS	Hardwired	Distribute DCS input signals to PAS
PACS	PS	Hardwired	Actuator checkbacks for interlock functions
	SICS	Hardwired	Actuator checkbacks
	SAS	Hardwired	Actuator checkbacks
	PAS	Data	Actuator checkbacks
Sensors/ Black Boxes	SCDS	Hardwired	Send signals to the DCS for distribution to multiple DCS subsystems
	PAS	Hardwired	Send non-safety related signals to the DCS if only needed in PAS

Table 7.1-9—Prioritization Scheme Analysis
Sheet 1 of 2

Signal Types	Effect on PACS	Effect on Plant
Concurrent and Conflicting	The PACS module provides the actuation for the actuation signal with the highest priority. For concurrent and conflicting SICS commands (SICS open and close), the PACS module will not provide any actuation outputs. For other systems' commands the PACS module will be configured to either an OPEN/ON priority or CLOSE/OFF priority depending on the actuator.	The actions of the system with the highest priority are executed. Priority is defined such that safety-related actions have higher priority than non-safety, therefore the plant will continue to operate in a safe manner.
Non-concurrent	For PS, SAS, and PAS signals: The PACS module provides the actuation for the actuation signal present at that moment in time. Once the actuation signal is removed, the PACS removes its actuation signal to the actuator. For SICS signals: The PACS module provides the actuation for the SICS actuation signal. The PACS latches its output to provide an actuation signal until the device reaches its final limit position. Once the device reaches its final limit position the PACS unlatches its output and does not provide an actuation signal. During this time period when the PACS module output is latched, if the SICS actuation signal is removed, the PACS module will continue provide an actuation signal until the device reaches its final limit position. During this time period when the PACS module output is latched and the SICS actuation signal is removed, if the PACS receives a conflicting SICS actuation signal, then the PACS module will stop its previous actuation and provide actuation signal for the new SICS actuation signal.	The actions of the system providing the actuation signal present at that moment in time are executed. If this action brings the plant to a unsafe state, then once the plant reaches a protection setpoint, the higher priority safety system shall provide an concurrent signal to maintain the plant in a safe state.

07.01-54

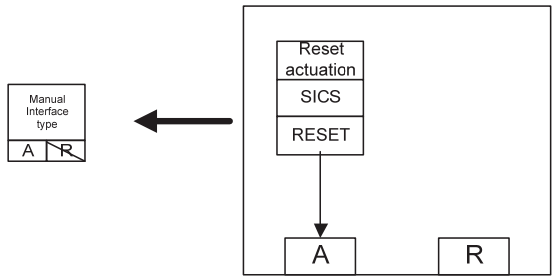
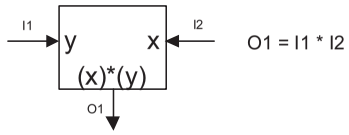
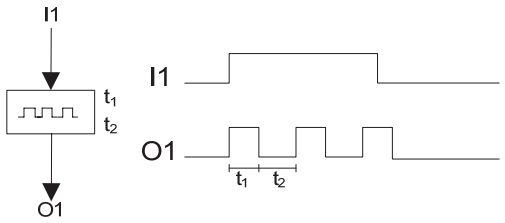
Table 7.1-9—Prioritization Scheme Analysis
Sheet 2 of 2

Signal Types	Effect on PACS	Effect on Plant
Combination of Both Concurrent and Non-concurrent (e.g. Overlapping signals for a period of time)	For the time period where the signals are concurrent, the PACS module behaves as described in the concurrent and conflicting signals section. For the time period where the signals are non-concurrent the PACS module behaves as described in the non-concurrent signal section.	For the time period where the signals are concurrent and conflicting: The actions of the system with the highest priority are executed. Priority is defined such that safety-related actions have higher priority than non-safety, therefore the plant will continue to operate in a safe manner. For the time period where the signals are non-concurrent: The actions of the system providing the actuation signal present at that moment in time are executed. If this action takes the plant towards an unsafe state, then once the plant reaches a protection setpoint (before the unsafe state), the higher priority safety system shall provide an concurrent signal to maintain the plant in a safe state.

07.01-54

07.01-54

Figure 7.1-1—Chapter 7 Symbol Legend
Sheet 11 of 16

Symbols – Logic Figures	Definition
Manual Interface Block (Actuate only) 	Manual Interface Block Actuate Only
	Multiplication Function
	Continuous Pulse Function

REV 005
EPR3000-I1 T2

Figure 7.1-2—Distributed Control System Functional Architecture

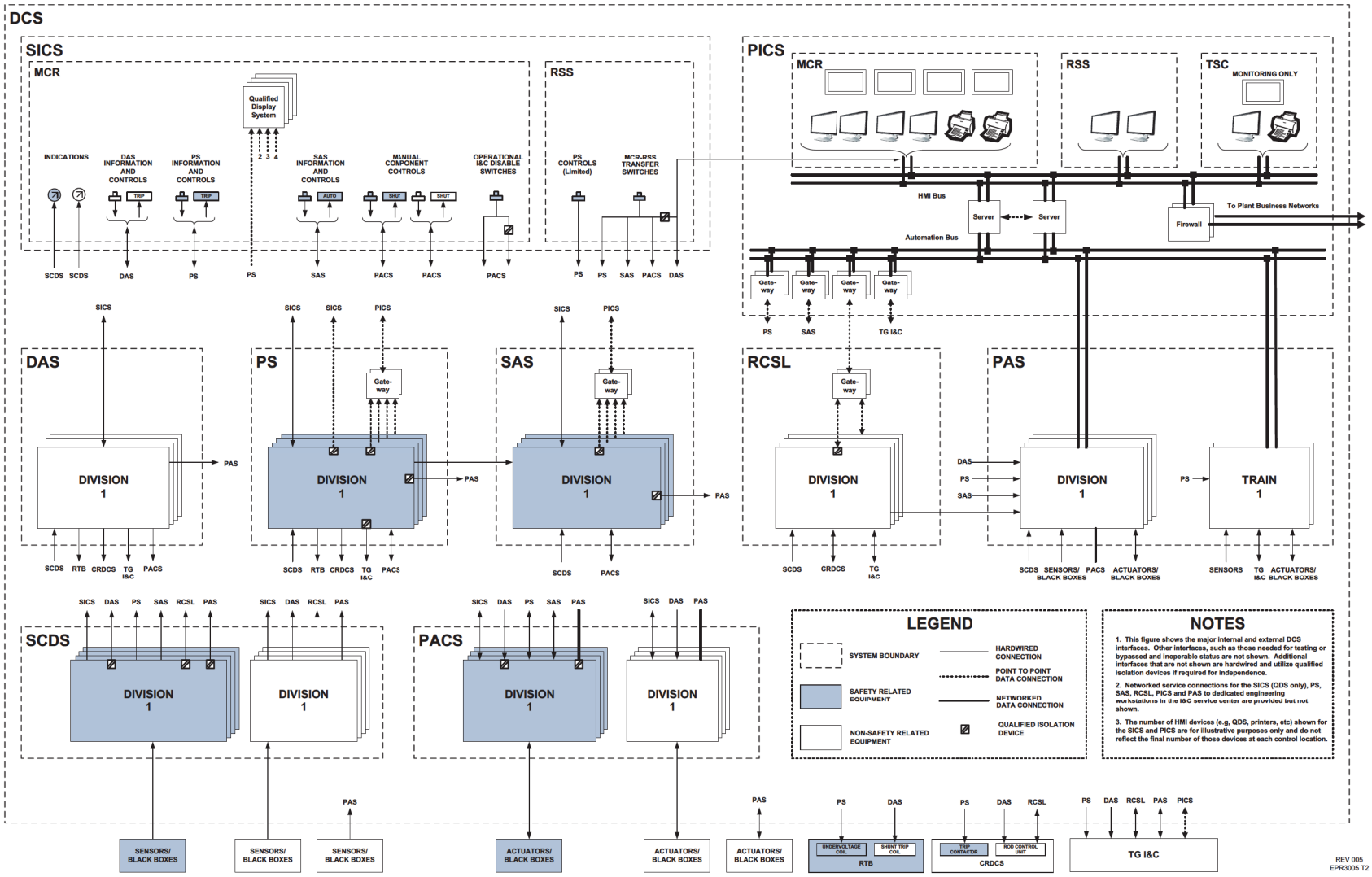
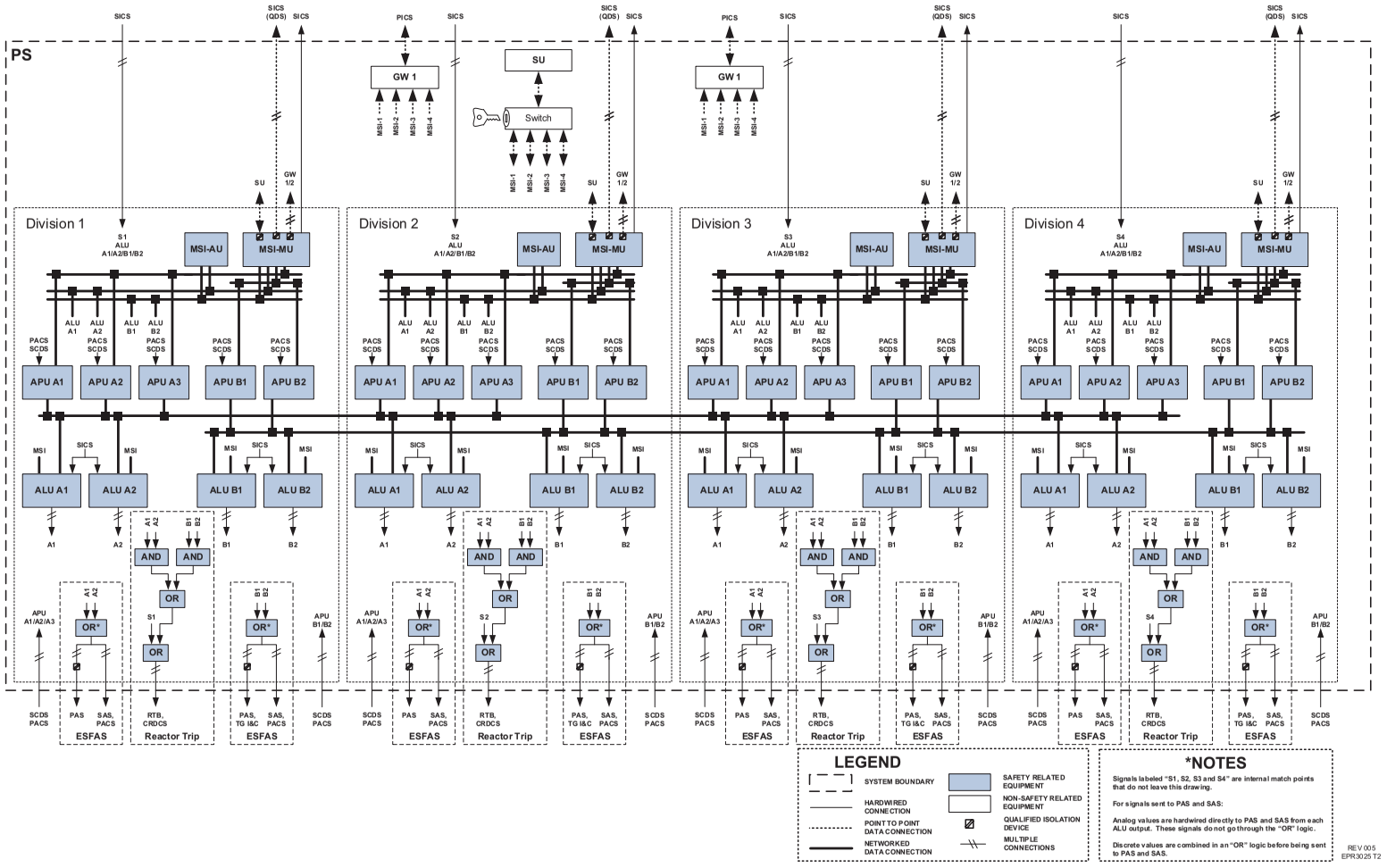


Figure 7.1-6—Protection System Architecture



07.01-54

Figure 7.1-8—Priority and Actuator Control System Architecture

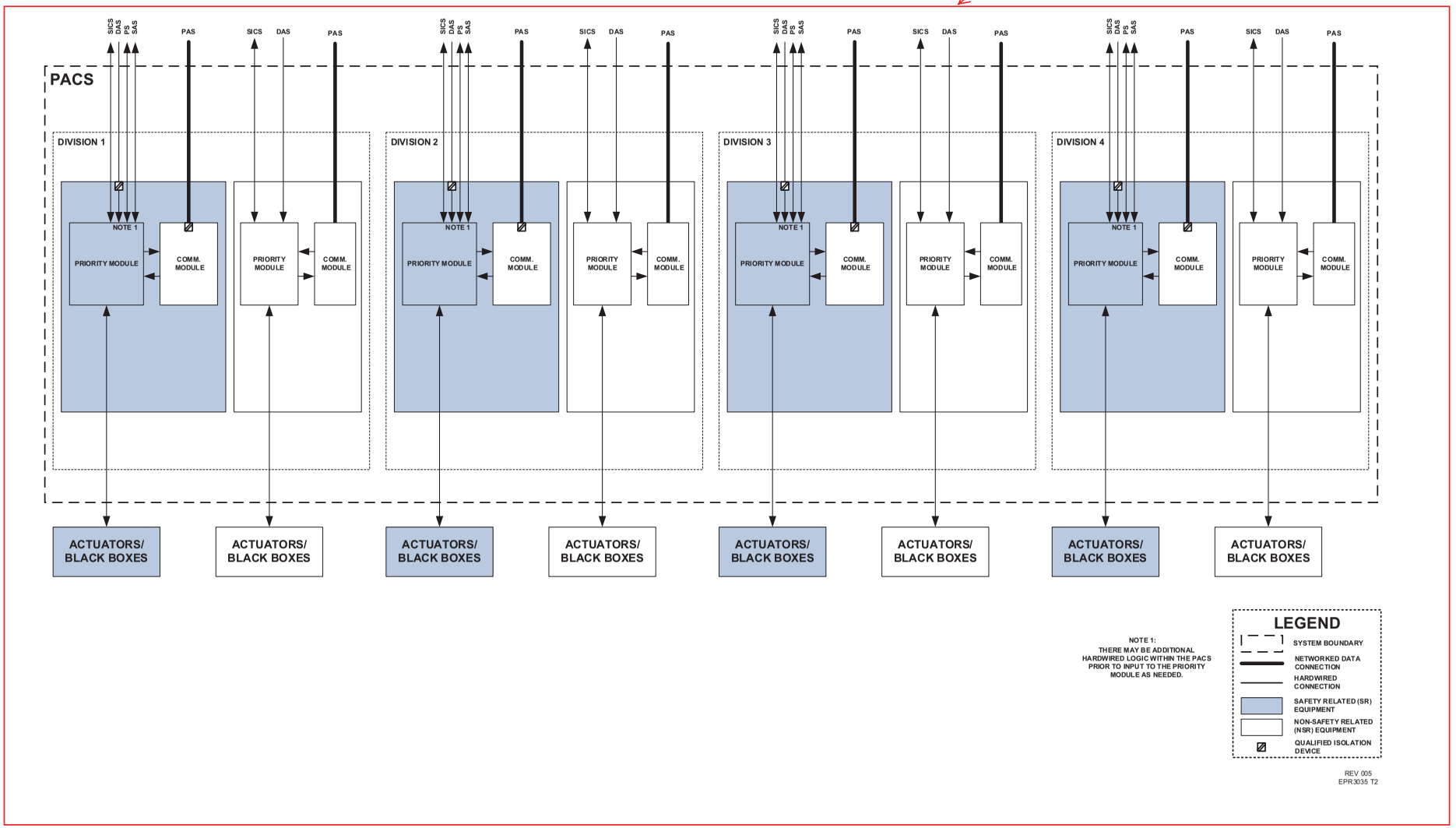
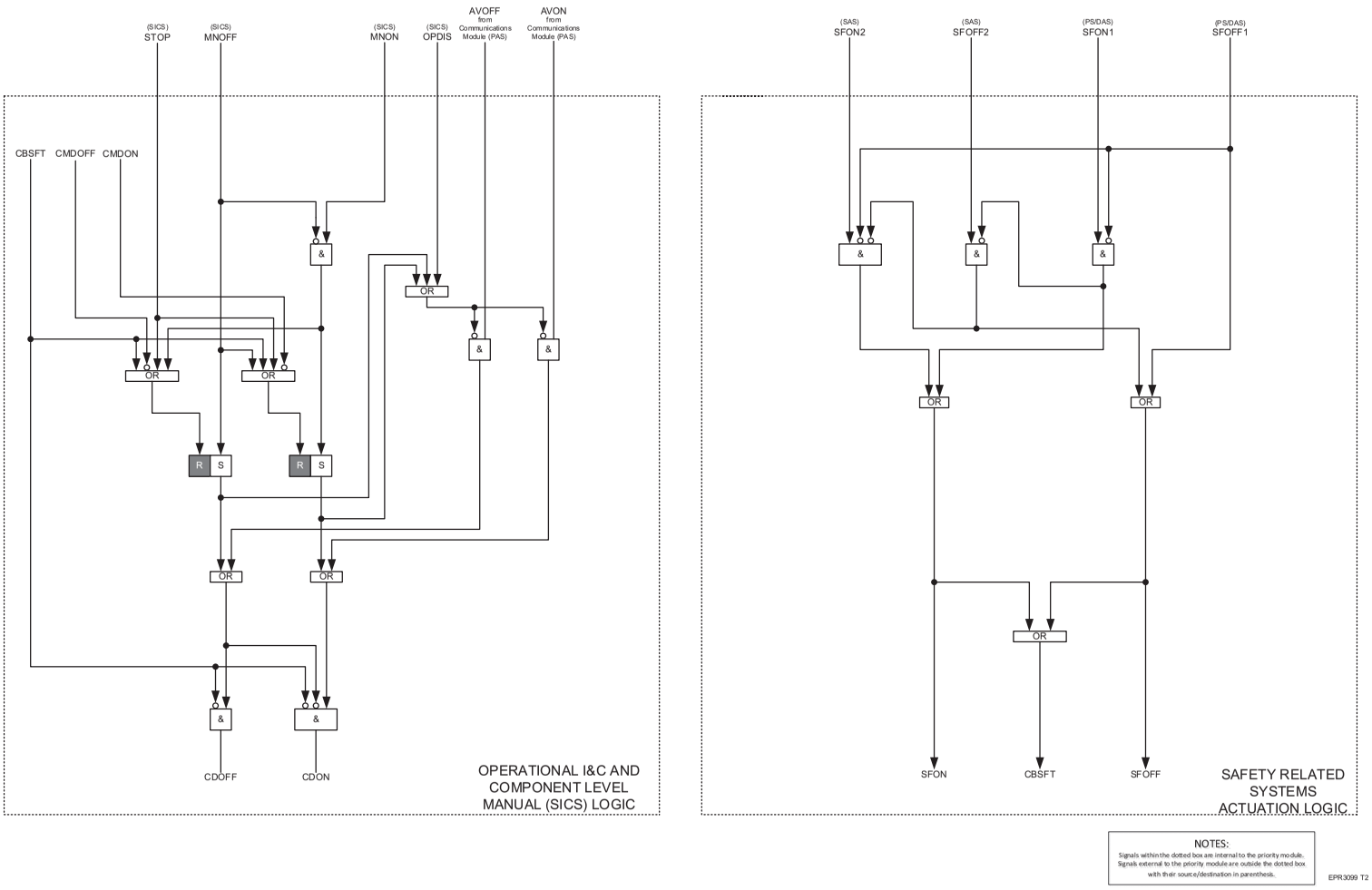


Figure 7.1-9—Deleted

07.01-54

Figure 7.1-21—PACS Priority Module Logic Diagram
Sheet 1 of 2



07.01-54

Figure 7.1-21—PACS Priority Module Logic Diagram
Sheet 2 of 2

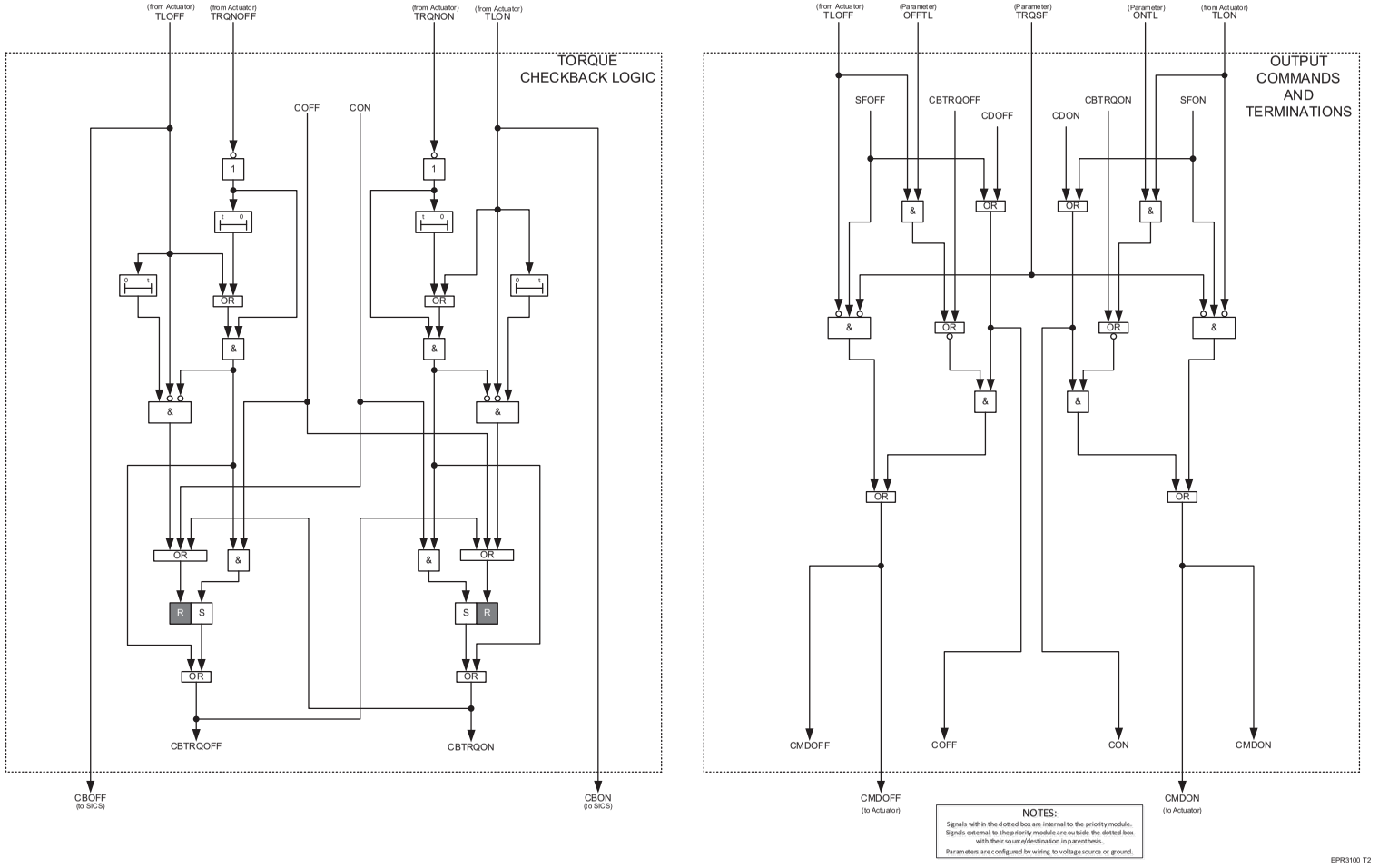
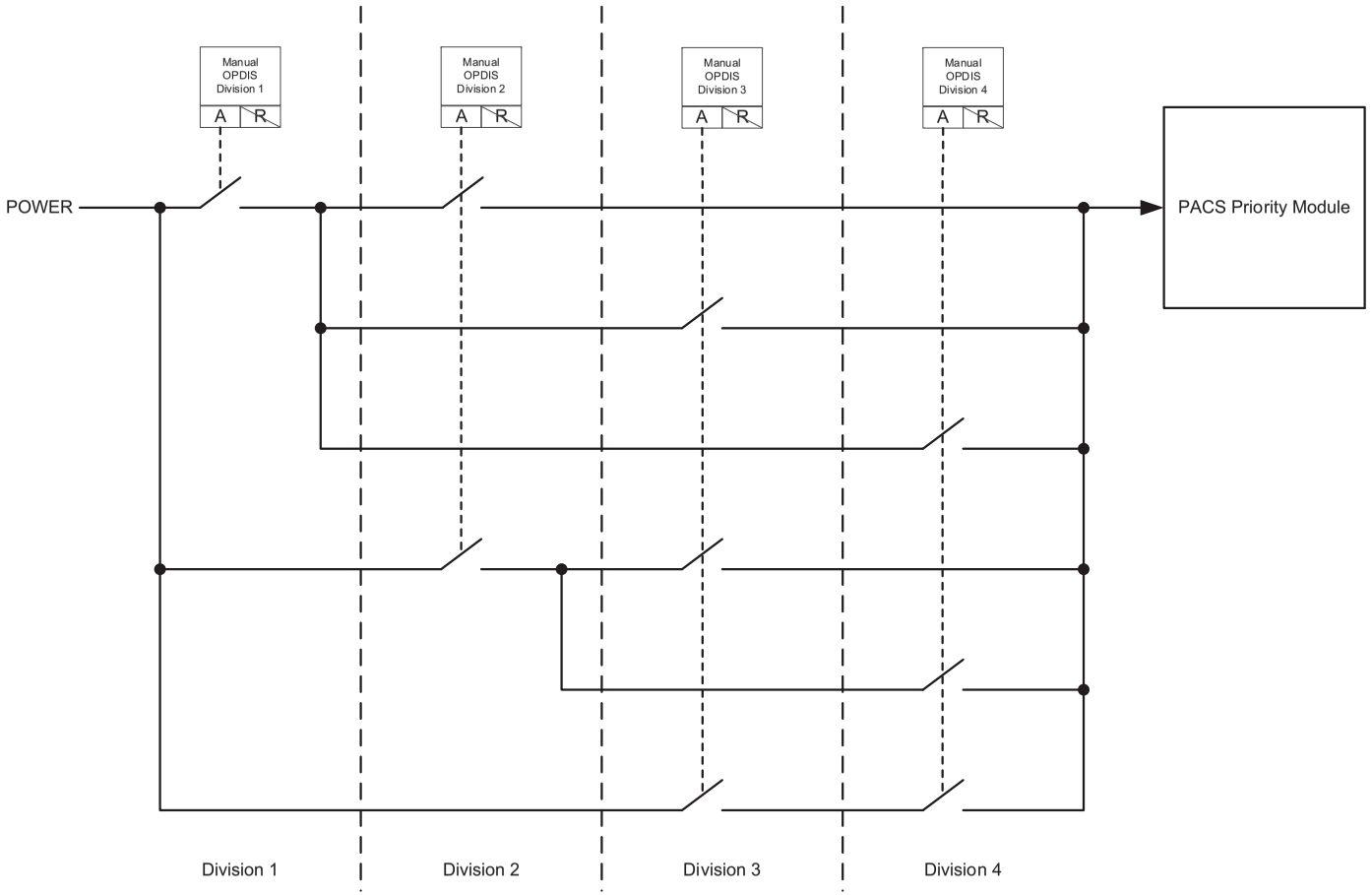


Figure 7.1-30—Operational I&C Disable Switch Configuration



Note: The connections in this figure are "make", not "break"

EPR3097 T2

- RCP bus breaker open position.
- First RCP speed measurement less than or equal to a setpoint (90 percent).
- Second RCP speed measurement less than or equal to a setpoint (90 percent).

07.01-54

When "RCP OFF" signals are generated for all four pumps, a delay time is started. The time delay function block is used to consider the RCP coast down time before validating the permissive and considering the RCPs totally off. After the delay time has expired, the permissive is validated.

This permissive is P-AUTO with respect to validation and inhibition.

Figure 7.2-34—P15 and P7 Permissive Logic illustrates the logic for the P7 permissive.

7.2.1.3.6 P8 Permissive

The P8 permissive defines the shutdown state with all rods in (ARI).

Rod cluster control assembly (RCCA) analog rod position sensors are acquired in four different electrical divisions. For each division, when all rods in the shutdown banks are less than the P8 permissive setpoint (two inches), a signal is generated. When two-out-of-four of divisions indicate all rods in, the permissive is validated.

This permissive is P-AUTO with respect to validation and inhibition.

Figure 7.2-30—P8 Permissive Logic illustrates the logic for the P8 permissive.

7.2.1.3.7 P12 Permissive

The P12 permissive facilitates plant heatup and cooldown by disabling certain ESF functions.

Pressurizer pressure (NR) measurements are compared to the P12 permissive setpoint (2005 psia). When three-out-of-four of the measurements are less than the setpoint, the operator is prompted to manually validate the permissive.

This permissive is P-MANU with respect to validation and P-AUTO with respect to inhibition.

Figure 7.2-31—P12 Permissive Logic illustrates the logic for the P12 Permissive.

7.2.1.3.8 P13 Permissive

The P13 permissive defines when SG draining and filling operations are allowed.

Actuation orders are sent from the PS to the PACS priority module associated with each actuator required for the function. The exception to this is the turbine trip function. The actuation order is transmitted via hardwired connections to the turbine-generator instrumentation and control system (TG I&C) and does not involve the PACS. The connections between the PS and TG I&C are shown in Figure 7.1-27. The PS and the PACS are discussed in Section 7.1. The TG I&C system is described in Section 10.2.

The safety automation system (SAS) performs closed loop automatic controls of certain ESF systems following their actuation by the PS. These controls are described in Section 7.3.1.3. The SAS also performs functions for essential auxiliary support (EAS) systems. These are systems that provide support to the ESF systems. These controls are described in Section 7.3.1.4. The list of functions performed by the SAS is described in Table 7.1-5. The other functions described in Section 7.3 are done by the PS. The SAS is described in Section 7.1.

The capability for manual system-level ESF actuations is available to the operator through the safety information and control system (SICS) in the MCR. These manual actuations are acquired by the ALUs in the PS and combined with the automatic actuation logic. The manual actuations are described with the corresponding automatic function in Section 7.3.1.2.

The capability for component-level control of ESF system actuators is available to the operator on both the PICS and the SICS in the MCR. Commands from the PICS are processed by the PAS and sent to the PACS for prioritization. Commands from the SICS are sent directly to the PACS for prioritization. SICS is the safety-related actuation path and PICS is the non-safety-related actuation path. The manual system-level ESF actuation sequence is shown in Figure 7.3-1 (Sheet 2). The manual actuations are described with the corresponding automatic function in Sections 7.3.1.2.

For an extra borating system (EBS) malfunction event, the component-level controls on SICS are credited to terminate EBS. For the failure of small lines carrying primary coolant outside the Reactor Containment Building (Section 15.0.0.3.5), component-level controls from SICS are credited to isolate the failed line. Operator actions credited in mitigating accidents are addressed in Section 15.0.0.3.7.

07.01-54

The capability for manual reset of sense and command ESF actuation outputs is provided on the SICS. Not all ESF actuations require a manual reset. The automatic safety related actuation functions' output signals must be reset manually unless there is justification for the functions' signals being reset automatically. There are cases where a sense and command output is cleared after the PS determines that the initiating condition has cleared. The reset functionality related to each ESF actuation is described in Section 7.3.1.2. Further description of the operation of the SICS is

EFWS actuation based on low SG level is performed on a per SG basis. The actuation order is generated when two of four SG level (WR) measurements (SG pressure sensors are used to improve the accuracy of the level measurement) are below the Min2p setpoint in any one SG. Only the EFWS train corresponding to the SG with the low level condition is actuated.

EFWS actuation based on LOOP and SIS actuation is performed concurrently on all SGs. Generation of the SIS actuation signal is described in Section 7.3.1.2.1. Generation of the LOOP signal is described in Section 7.3.1.2.12.

In both cases, EFWS actuation is bypassed when hot leg temperature is below the P13 permissive setpoint. The bypass is automatically removed above the P13 permissive setpoint. Generation of the P13 permissive signal is discussed in Section 7.2.1.3.8.

When EFWS actuation occurs due to a low SG level, the sense and command actuation output is reset automatically when the SG level returns above the Min2p setpoint. This is done so that the safety-related SG level control loop, performed by the SAS, can control the actuators needed to maintain the correct water level in the SG. Additionally, the capability for manual reset of the EFWS actuation signal is available, on a per train basis, from the SICS in the MCR and the RSS. The manual reset does not result in stopping the EFWS actuation; it allows the operator to take further manual actions to stop the actuation.

07.01-54

When EFW actuation occurs due to LOOP and SIS actuation, the PS sends a pulse signal of limited duration to start the actuation. The duration of the pulse is long enough for the intended actions of the execute features to go to completion. The pulse function logic block is used to maintain the actuation signal until the actuator reaches its final position. Then the actuation signal is removed, and the EFW SG Level Control function maintains the level. The safety function is completed once the EFW is initiated, and the valves and pumps are in their final position/state. No reset is needed in this case, as the SG water level is already above the Min2p setpoint when the EFW actuation occurs and the safety-related SG level control loop can immediately take control of the actuators.

The EFWS SG level control and EFWS pump flow protection functions provide the EFWS control valves with a position correction signal to move the valves in the close or open direction as needed. The actual SG level and EFWS pump discharge flow are compared to their respective setpoints. A proportional and integral (PI) step controller sends a close or open signal, depending on the valve position, to maintain the SG level and EFWS pump discharge flow parameters at their respective setpoints.

The safety-related closed loop control for SG water level following EFWS actuation is performed by the SAS. When EFWS actuation occurs, the PS signals the SAS to initiate the closed loop control. Separately, during SG water level control by the SAS,

07.01-54

time delay initiated by RT signal. The time delay logic block is used to isolate all main feedwater (i.e., SSS Isolation) if a high SG level (SG Level > Max0p) is present after a RT and MFW full load isolation (both on SG Level > Max1p) has occurred. The time delay is used to provide a wait time after a RT and MFW full load isolation, for the SG level to decrease below the Max0p setpoint. If after the time delay expires, the SG level is above the Max0p setpoint, it is necessary to isolate all main feedwater. The SSS isolation is performed only on a SG in which the level remains above the Max0p setpoint. This initiation signal is bypassed when hot leg temperature is below the P13 permissive setpoint. The bypass is automatically removed when hot leg temperature is above the P13 permissive setpoint. Generation of the P13 permissive signal is discussed in Section 7.2.1.3.8.

Following a main steam or feedwater system piping failure, a complete feedwater isolation of the MFW train feeding the affected SG is desirable. In this case, MFW full load isolation occurs on all four SGs because of the reactor trip on either SG pressure drop or on SG pressure < Min1p. A MFW SSS isolation of the affected SG will occur on a more severe SG pressure drop (to mitigate fast depressurizations) or on SG pressure < Min2p (to mitigate slower depressurizations). The logic to initiate MFW isolation on SG pressure drop is the same as that described for main steam isolation on SG pressure drop described in Section 7.3.1.2.7, except that the variable low setpoint for SSS isolation is maintained below the RT and main steam isolation setpoint. The actuation order for SSS isolation due to SG pressure < Min2p is generated when two out of four SG pressure measurements on any one SG are below the Min2p setpoint. There is no operating bypass associated with SSS isolation on SG pressure drop. SSS isolation on SG pressure < Min2p is bypassed when RCS pressure is below the P12 permissive setpoint. The bypass is automatically removed when RCS pressure is above the P12 permissive setpoint. Generation of the P12 permissive signal is discussed in Section 7.2.1.3.7.

An actuation order is generated for SSS isolation when two-out-of-four PS divisions detect high containment pressure. Either two-out-of-four equipment compartment pressure measurements exceeding the Max1p setpoint, or two-out-of-four service compartment pressure (NR) measurements exceeding the Max2p setpoint results in SSS isolation. There are no operating bypasses associated with SSS isolation on high containment pressure.

The capability for manual system-level isolation of MFW on a per-train basis is provided on the SICS in the MCR. This manual system-level initiation isolates both full load and SSS lines on the desired SG. Two manual system-level isolation controls are provided per MFW train. Either of the two controls isolates the MFW train.

The capability for component-level control of the MFW actuators is available to the operator on both the PICS and the SICS in the MCR.

P17 permissive setpoint. Generation of the P17 permissive signal is discussed in Section 7.2.1.3.12.

The capability for manual system-level initiation of CVCS charging isolation is provided on a per-division basis on the SICS in the MCR. One manual system-level isolation control is provided for PS Division 1, and one control is provided for PS Division 4.

The capability for component-level control of the CVCS actuators for CVCS charging isolation is available to the operator on both the PICS and the SICS in the MCR.

A manual reset of the sense and command outputs is not required for the CVCS charging isolation function. The outputs are automatically reset when the level measurements return below the appropriate setpoint. The pulse function logic block provides a minimum actuation output time to maintain an actuation signal, until the actuators reach their final position. A pulse order is used to provide assurance that the actions of the execute features go to completion. The automatic reset of the sense and command outputs does not result in change of state of the isolation actuators; it allows the operator to take further manual actions to change the state of individual actuators.

07.01-54

The functional logic for CVCS charging isolation is shown in Figure 7.3-21—CVCS Charging Isolation.

7.3.1.2.11 CVCS Isolation for Anti-Dilution

To mitigate the risk of dilution of the RCS boron concentration, a CVCS isolation is required to secure potential dilution flow paths. This function provides protection during all plant conditions by using different combinations of input signals depending on the current plant state. The function is divided as follows:

- Power operation (above the P8 permissive).
- Shutdown conditions with RCPs in operation (below the P8 permissive and above the P7 permissive).
- Shutdown conditions without RCPs in operation (below the P7 permissive).

An online calculation of the boron concentration in the RCS is performed during power operation based on the boron concentration measurement in the CVCS charging line and the measured CVCS charging flow. The calculated boron concentration is compared to a fixed setpoint corresponding to the critical boron concentration of the core at hot zero power with the highest worth rod not inserted. The boron concentration calculation is performed according to the following:

The EDG actuation function is implemented in the PS architecture differently than the remainder of the ESF actuation functions. The three phases of voltage measurement for any one electrical division are acquired by the corresponding PS division. The processing and actuation of the related EDG are also carried out completely within the same PS division. For the actuation of any one EDG, redundancy within the PS is obtained by utilizing the functionally independent sub-systems within each division. Both sub-systems within a division acquire the voltage measurements and either sub-system can actuate the same EDG. For this function, the two ALU within a sub-system are combined in a "functional AND" logic. The result of the "functional AND" logic in each sub-system are combined in a "functional OR" logic so that either sub-system within a division can start the corresponding EDG.

07.01-54

There are two types of uses for the time delay logic block in the EDG Actuation function. The first time delay is for preventing spurious starts of the EDG on dips in the voltage. This is the time delay that is paired with each threshold logic block on the EDG Actuation logic. The operator receives an alarm if the voltage degrades for longer than the first set of time delays. The second time delay in the downstream logic allows the operator time to correct the degraded voltage condition once the operator has received an alarm. If the operator does not correct the degraded voltage condition by the time period of the second time delay, then the EDG will be started and loaded so that the electrical bus is on a known good source.

The capability for manual system-level start-up of EDGs on a per-EDG basis is provided on the SICS in the MCR. Two manual system-level controls are provided per EDG. Either of the two controls starts the desired EDG.

The capability for component-level control of the EDG is available to the operator on both the PICS and the SICS in the MCR.

The sense and command outputs for EDG actuation can be manually reset from the SICS in the MCR. Reset of the sense and command outputs does not result in change of state of the actuators; it allows the operator to take further manual actions to change the state of individual actuators.

The functional logic used to generate an EDG actuation order is shown in Figure 7.3-23—EDG Actuation.

7.3.1.2.13 Pressurizer Safety Relief Valve Opening (Brittle Fracture Protection)

The integrity of the reactor pressure vessel (RPV) must be protected under all plant conditions. During normal power operation, overpressure protection is provided by three spring-loaded PSRVs. At low coolant temperatures, the cylindrical part of the vessel could fail by brittle fracture before the design pressure of the RCS is reached. In cold operating conditions, low-temperature overpressure protection (LTOP) is provided by opening two of the three PSRVs via redundant electrical solenoid valves.

The functional logic for automatic SG isolation is shown in Figure 7.3-25—SG Isolation (Div. 1&2) and in Figure 7.3-26—SG Isolation (Div. 3&4).

7.3.1.2.15 Reactor Coolant Pump Trip

In case of a SBLOCA, RCPs are tripped when conditions indicate that two-phase flow is present. This is done because the RCPs may subsequently be lost due to cavitation or operation in a degraded environment. Forced convection of the two-phase flow increases the mass lost via the break. If the RCPs are permitted to operate for an extended period of time in this condition and then are shut down, an inadequate core cooling condition may occur due to insufficient liquid inventory as the two phases separate. For this reason, an automatic RCP pump trip is provided early after two-phase flow is indicated, while the void fraction is still relatively low, to enhance long term accident mitigation and minimize the potential for RCS mass depletion.

Additionally, the RCPs are tripped on a containment isolation (stage 2) signal.

The operation of the RCPs is described in Section 5.4.1.

The U.S. EPR design uses the following initiating conditions to actuate RCP trip:

- ΔP across RCP < Min1p and SIS actuation signal generated.
- Containment isolation (stage 2) signal generated.

The RCP trip based on differential pressure across the RCP results from one of two ΔP measurements below the Min1p setpoint on any two-of-the-four RCPs. A safety injection signal must also be present in addition to the low ΔP condition for this actuation to occur. This reduces the possibility of a spurious RCP trip.

The parameters that result in RCP trip due to a containment isolation (stage 2) are described in Section 7.3.1.2.9.

When the conditions for RCP trip are satisfied, orders are issued to open the circuit breakers that supply power to each RCP. When the orders are issued, a time delay begins. The time delay logic block is used to delay the opening of the redundant RCP circuit breaker so that simultaneous opening of RCP circuit breakers does not cause an excessive voltage surge. When the time delay expires, an order is issued to trip the corresponding bus supply circuit breaker upstream of the RCP circuit breaker to remove power from the RCP.

07.01-54

There are no operating bypasses associated with the RCP trip function.

The capability for manual system-level RCP trip on a per-pump basis is provided to the operator on the SICS in the MCR. Two system-level initiation controls are provided for each pump. Either of the controls will trip the desired RCP.

in a change of state of the actuators; it allows the operator to take further actions to manipulate individual components as may be necessary to follow plant operating procedures.

The functional logic for MCR air conditioning system isolation and filtering is shown in Figure 7.3-28—MCR Air Conditioning System Isolation and Filtering.

7.3.1.2.17 Turbine Trip on Reactor Trip Initiation

A turbine trip (TT) is required following any RT in order to avoid a mismatch between primary and secondary power, which would result in excessive RCS cooldown with a potential inadvertent return to critical conditions and a power excursion.

07.01-54

A short delay is implemented between the RT activation and the TT demand to limit the overpressure effect. The time delay logic block is used for a loss of flow event (loss of one RCP) at 100% power that results in a Reactor Trip on Low-Low RCS Flow Rate (Figure 7.2-11). The safety analysis assumes that a turbine trip LOOP occurs and results in the loss of the three remaining operating RCPs. The time delay duration is the minimum time to delay the loss of the remaining three RCPs, to allow the trip to reduce power sufficiently, such that the loss of the remaining three RCPs does not challenge DNB limits.

The U.S. EPR design uses the following initiating condition to actuate the TT:

- RT Initiation.

The various conditions that lead to RT are described in Section 7.2.

Each divisional TT signal from the PS is sent to the TG I&C via a hardwired, isolated connection. A two-out-of-four logic is performed in each division of the TG I&C on the four PS divisional signals. These connections between the PS and TG I&C are shown in Figure 7.1-27.

The capability for manual system-level initiation of TT is provided on the SICS in the MCR. Four manual system-level initiation controls are provided; the activation of any two of the four results in turbine trip.

The capability for component-level control for the TT function is available to the operator on both the PICS and the SICS in the MCR.

Manual reset of the sense and command output for TT is available from the SICS in the MCR. A reset of the sense and command output does not result in a change of the state of the actuators; it allows the operator to take further actions to manipulate individual components as may be necessary to follow plant operating procedures.

Common 2.a and 2.b headers. The functional logic is shown in Figure 7.3-33—CCWS Common 1.b Automatic Backup Switchover of Train 1 to Train 2 and Train 2 to 1.

Common 2.b Automatic Backup Switchover of Train 4 to 3

~~The CCWS has a safety-related function to remove heat from safety-related components (GDC 44).~~ The safety-related function to perform an automatic switchover from Train 4 to Train 3 verifies that the CCWS is capable of fulfilling its safety-related function to remove heat from safety-related components on the CCWS Common 2.a and 2.b headers. The functional logic is shown in Figure 7.3-33—CCWS Common 1.b Automatic Backup Switchover of Train 1 to Train 2 and Train 2 to 1.

Emergency Temperature Control

~~The CCWS has a safety-related function to remove heat from safety-related components (GDC 44).~~ The safety-related function to control the CCWS heat exchanger (HX) outlet temperature is required to maintain the temperature of the cooling water within its limits. This verifies that the CCWS is capable of fulfilling its safety-related function to remove heat from safety-related components. The functional logic is shown in Figure 7.3-34—CCWS Emergency Temperature Control.

07.01-54

The continuous pulse function logic block is used to close the heat exchanger bypass valve 10 percent of its 0-100 percent range at 1 minute intervals. This provides a gradual opening of the heat exchanger bypass valve and, therefore, a gradual cooling to the heat exchanger. The continuous pulse function block is initiated by a high heat exchanger temperature, and the continuous pulse is ended if the heat exchanger temperature falls below the high setpoint or the heat exchanger bypass valve is in the fully closed position. This provides assurance that the actuation signal is maintained until the execute features go to completion.

Emergency Leak Detection

~~The CCWS has a safety-related function to remove heat from safety-related components (GDC 44).~~ The safety-related function for emergency leak detection maintains the required cooling water inventory that supports the safety-related function to remove heat using indications to detect leaks and isolate them (GDC 44). The functional logic is shown in Figure 7.3-35—CCWS Emergency Leak Detection.

Emergency Leak Detection - Switchover Valves Leakage or Failure

~~The CCWS has a safety-related function to remove heat from safety-related components (GDC 44).~~ The safety-related function for switchover valve leakage or failure isolates the CCWS trains from their common headers so that each train is able to provide their corresponding LHSI HX with the required flow for heat removal. Removing heat from the LHSI HX is a safety-related function. The functional logic is

recirculation air flow as required to maintain ambient temperature and air quality (via filtration) within applicable limits for safety-related equipment located within the Safeguard Building areas and rooms. The pulse function logic block provides a minimum actuation output time to maintain an actuation signal, until the actuators reach their final position. A pulse order is used to provide assurance that the actions of the execute features go to completion. The functional logic is shown in Figure 7.3-48—SBVSE Supply and Recirculation-Exhaust Air Flow Control.

07.01-54

Supply Fan Safe Shut-Off

~~The SBVSE has a safety-related function to ventilate and maintain acceptable ambient temperature in the Safeguard Building areas and rooms ventilated by the system (GDC 4, GDC 17).~~ An inadvertent stopping of the supply fan, due to a spurious system action, may cause the SBVSE for a given division to become inoperable. Therefore, to mitigate the risk of system spurious actions, this function is to be designated as safety-related (IEEE 603). The functional logic is shown in Figure 7.3-49—SBVSE Supply Fan Safe Shut-Off.

Recirculation Fan Safe Shut-Off

~~The SBVSE has a safety-related function to ventilate and maintain acceptable ambient temperature in the Safeguard Building areas and rooms ventilated by the system (GDC 4, GDC 17).~~ An inadvertent stopping of the recirculation/exhaust fan, due to a spurious system action, may cause the SBVSE for a given division to become inoperable. Therefore, to mitigate the risk of system spurious actions, this function is to be designated as safety-related (IEEE 603). The functional logic is shown in Figure 7.3-50—SBVSE Recirculation Fan Safe Shut-Off.

Exhaust Fan Safe Shut-Off

~~The SBVSE has a safety-related function to ventilate and maintain acceptable ambient temperature in the Safeguard Building areas and rooms ventilated by the system (GDC 4, GDC 17).~~ An inadvertent stopping of the exhaust fan, due to a spurious system action, may cause the SBVSE for a given division to become inoperable. Therefore, to mitigate the risk of system spurious actions, this function is to be designated as safety-related (IEEE 603). The functional logic is shown in Figure 7.3-51—SBVSE Exhaust Fan Safe Shut-Off.

Supply Air Temperature Heater Control

The SBVSE has a safety-related function to ~~ventilate and maintain acceptable ambient temperature in the Safeguard Building areas and rooms ventilated by the system (GDC 4, GDC 17). The Supply Air Temperature Heater Control function supports this system safety function by~~ maintain~~ing~~ supply air temperature (downstream of heaters) as required to maintain ambient temperature within applicable limits for safety-related

control based on which electrical division provides power to the valves (i.e., valves powered by electrical Division 1 are controlled by SAS Division 1). The closed position indications of the CIVs on Common 1b are used to allow opening of the CIVs on Common 2b, and the closed position indication of the CIVs in Common 2b are used to allow the opening of the CIVs on Common 1b.

Redundant SAS controllers are provided in each division, and redundant networks are used between the divisions so that no single failure within the SAS can result in inadvertent connection or closure of redundant CCWS trains. ~~Two SAS CU pairs are provided per division for this function, one SAS CU pair detects the CIV positions of one common header (1b) and provides the necessary actuations, the other SAS CU pair detects the CIV positions of the other common header (2b) and provides the necessary actuations.~~ Each valve is equipped with redundant open/closed position sensors so that a single sensor failure does not result in inadvertent connection of redundant CCWS trains. While each switchover valve is controlled by one SAS division, PACS modules in multiple divisions, acting on multiple solenoid devices, are required in order to change the position of a switchover valve. Therefore, a single PACS module failure does not result in inadvertent connection of redundant CCWS trains. For the CIV interlock, redundancy is obtained through the use of inner and outer CIVs, each controlled by a different division of SAS.

The single failure tolerance of the CCWS with respect to availability of the required cooling function is encompassed within the redundancy of the mechanical system design, as described in Section 9.2.2, and the two SAS CU pairs per division for the function.

07.01-54

The pulse function logic block is used so that once an operating common header is isolated, a momentary signal opens the standby common header and isolates the rest of the operating common header. This provides a momentary signal to switchover from an operating common header to the standby common header. The momentary signal's duration maintains an actuation signal, until the actuators reach their final position. A momentary signal is used to prevent concurrent and conflicting signals to the actuators between the CCWS RCP Thermal Opening function and the CCWS RCP Thermal Barrier Containment Isolation Valves Interlock for maintaining independence between the CCW trains feeding the RCP thermal barrier. A pulse order is used to provide assurance that a complete switchover between common headers occurs.

The following indications are provided to the operator relative to these interlocks:

- Indication of open or closed position of each interlocked valve.
- Alarm indicating position conflict between supply and return switchover valve of the same CCWS train relative to the same common header.
- Alarm indicating position conflict between CIVs of the same common header.

- Alarm indicating connection of two CCWS trains to the same common header.

7.6.1.2.6 IRWSTS Boundary Isolation for Preserving IRWST Water Inventory Interlock

The IRWST has a safety-related function to isolate the IRWST for purposes of preserving the IRWST water inventory to support the safety-related function of controlling core reactivity (via safety injection) by closing the IRWST isolation valves. This preserves IRWST inventory for long-term availability of safety injection, given a pipe failure in a connected non-safety related system. ~~The CCWS has a safety-related function to remove heat from safety-related components (GDC 44). The interlock function is required to verify that the two trains connected to their common headers remain separated and each are able to provide their corresponding LHSI HX with the required flow for heat removal. Removing heat from the LHSI HX is a safety-related function.~~ The functional logic is shown in Figure 7.6-4—IRWSTS Boundary Isolation for Preserving IRWST Water Inventory Interlock.

7.6.1.2.7 Safety Chilled Water System Interlocks

The SCWS has the following safety-related functions:

1. Transfer of heat loads from safety-related SSC to a heat sink under both normal operating and accident conditions,

2. Component redundancy for performance of safety functions assuming a single, active component failure coincident with the loss of offsite power,

3. The capability to isolate components, systems, or piping, if required, so system safety functions are not compromised.

These safety-related automatic switchover functions ensure that during a failure that prevents the train in service from transferring heat loads, the redundant train turns on to transfer the heat loads from the safety-related SSC. The pulse function logic block is used so that the circulating pumps are started and run to full speed, before the actuation signal is removed. A pulse order is used to provide assurance that the actions of the execute features go to completion. The time delay logic block is used to start the pumps in a sequenced fashion (one pump at a time); so that they are running at full speed before they are loaded to the system. The following automatic switchover functions verify that the SCWS is capable of fulfilling the safety-related functions in compliance with GDC 44:

07.01-54

- SCWS Train 1 to Train 2 Switchover on Train 1 Low Evaporator Flow:

  The functional logic is shown in Figure 7.6-5—SCWS Train 1 to Train 2 Switchover on Train 1 Low Evaporator Flow / Chiller Blackbox Internal Fault / SCWS Chiller Evaporator Water Flow Control / LOOP Re-Start Failure Interlock.

- SCWS Train 2 to Train 1 Switchover on Train 2 Low Evaporator Flow:

Table 3.3.1-1 (page 13 of 14)
DCS Sensors, Function Processors, Manual Actuation Switches, and Trip Actuation Devices

	COMPONENT	APPLICABLE MODES OR OTHER SPECIFIED CONDITIONS	REQUIRED NUMBER	CONDITIONS	SURVEILLANCE REQUIREMENTS
28.	P16 permissive Inhibitation	4	4	T	SR 3.3.1.8
30.	P16 permissive Validation	4	4	T	SR 3.3.1.8
31.	P17 permissive Validation	4(s)	4	T	SR 3.3.1.8
		5(s),6(s)	2	Y	SR 3.3.1.8
32.	Operational I&C Disable	1,2,3,4	4	T	SR 3.3.1.8
		5,6	2	V,W,X,Y,Z,AA	SR 3.3.1.8

(s) When PSRV OPERABILITY is required by LCO 3.4.11.

07.01-55

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

31. P17 Permissive Validation

There is one manual P17 Permissive Validation switch per division.

Four of four manual P17 Permissive Validation switches are required to be OPERABLE in MODE 4 when PSRV OPERABILITY is required by LCO 3.4.11, "Low Temperature Overpressure Protection (LTOP)":

Two of four manual P17 Permissive Validation switches are required to be OPERABLE in MODES 5 and 6 when PSRV OPERABILITY is required by LCO 3.4.11, "Low Temperature Overpressure Protection (LTOP)":

The manual P17 Permissive Validation switch is utilized to disable the following ESF functions:

- ESF 11.a: CVCS Charging Isolation on High-High Pressurizer Level,
- ESF 12.a: PSRV Opening - First Valve, and
- ESF 12.b: PSRV Opening - Second Valve.

07.01-55

32. Operational I&C Disable

During normal operation, the operational I&C disable switch on the SICS is set so that the PAS can send commands to the PACS. In this configuration, automatic commands from the non-safety-related Plant Automation System (PAS) override manual commands from the SICS because of the nature of the manual control logic in the PACS. The operational I&C disable switch disables PAS inputs, all other PACS inputs remain operational.

There is one manual Operational I&C Disable switch per division.

Four of four manual Operational I&C Disable switches are required to be OPERABLE in MODES 1, 2, 3, and 4.

Two of four manual Operational I&C Disable switches are required to be OPERABLE in MODES 5 and 6.

ANP-10309 — U.S. EPR Protection System Technical Report Markups

- The actuation signal is latched via a memory logic block with set-reset priority ~~function block~~ in the ALU to confirm completion of the function. (See Figure 7.1-1 of the U.S. EPR FSAR and the glossary of ANP-10310P.)~~.~~

- The ESF actuation signals of the redundant ALUs in each subsystem are combined in a hardwired “functional OR”; therefore, either of the redundant ALUs can actuate an ESF function. The result of the “functional OR” is an ESF actuation order.

8.2 *ESF Actuation Voting Logic*

Single failures upstream of the ALU layer that could result in an invalid signal being used in the ESF actuation are accommodated by modifying the vote in the ALU layer. Each ESF actuation function is evaluated on a case-by-case basis to determine whether the vote is modified toward actuation or no actuation. In cases where inappropriate actuation of an ESF function could challenge plant safety, the function is modified toward no actuation. Otherwise, the function is modified toward actuation. The EDG Actuation and MCR Air Conditioning System Isolation and Filtering functions are the only ESF actuation functions that are modified towards actuation. All other ESF actuation functions are modified towards no actuation. The concept of modification toward actuation is described in Section 7.2. The concept of modification toward no actuation based on the number of input signals to the voting function block that carry a faulty status is as follows~~:~~.

Table 8-1—Modification of Voting Logic Towards No Actuation~~ESF Actuation Voting Logic~~

Voting Type	Faulty Inputs	Result
2 out of 4 3 out of 4	0	2 out of 4 3 out of 4
	1	2 out of 3
	2	2 out of 2
	3	No Actuation
	4	No Actuation
2 out of 3	0	2 out of 3

ANP-10315 —U.S. EPR Surveillance Testing and TELEPERM XS Self-MonitoringTechnical Report Markups

For certain functions (e.g. CCWS RCP thermal barrier containment isolation valves interlock), an inoperable division may put the system in an undesirable state for normal operation. Therefore, testing procedures are implemented to verify that the valves in the system are in the proper position to ensure continued system operation, before the test is executed. For systems that are fed by two redundant trains, the system is manually aligned to feed from trains that are not under test, while the redundant train is being tested.

2.2.5.1.2 ~~ESFAS~~ "Go" ADOT

The go portion of the ~~ESFAS~~ ADOT overlaps the no-go test in the priority logic of the PACS and includes the switchgear and the actuator itself. The go tests are performed on a per-actuator basis (i.e., each actuator is operated individually). This testing consists of exercising the actuator from the operator's normal human machine interface (HMI) in the main control room (MCR). The operator takes a manual action from the PICS to initiate operation of the actuator. The signal is transferred from the PICS to the PAS and then to the PACS priority logic via the PACS communication module. The priority logic then provides an output to the switchgear, and the actuator responds accordingly. The time stamping capabilities of the PAS are used to capture the time of the actuation output and the time that indication is received that the actuator has responded. The nature of feedback to PAS that the actuator has completed its action depends on the type of actuator and the maintenance procedures used by the plant operator. Typically, limit switches are used to indicate valve actions and either pump speed or flow measurements are used to determine that a pump has achieved its rated speed or flow. In this way, both the functionality and response time of each component downstream of the PACS is verified. The Operational I&C Disable switches are verified periodically (every 24 months) as part of the ADOT. Figure 2-6 shows the concept for the go test portion of ADOT.

07.01-55