ArevaEPRDCPEm Resource

From: WILLIFORD Dennis (AREVA) [Dennis.Williford@areva.com]
Sent: Friday, February 01, 2013 9:02 PM
To: Snyder, Amy
Cc: DELANO Karen (AREVA); LEIGHLITER John (AREVA); ROMINE Judy (AREVA); RYAN Tom (AREVA); TOLLEY Tracey (AREVA); VANCE Brian (AREVA); WELLS Russell (AREVA); WILLS Tiffany (AREVA); MEACHAM Robert (AREVA); Canova, Michael
Subject: Advanced Response to U.S. EPR Design Certification Application RAI No. 555 (6611), FSAR Ch. 7, Question 07.01-53
Attachments: RAI 555 Advanced Response Q 07.01-53 US EPR DC.pdf

Amy,

Attached is an Advanced Response to RAI 555, Question 07.01-53 in advance of the final response date of April 1, 2013.

To keep our commitment to send a final response to this question by the commitment date, we need to receive all NRC staff feedback and comments no later than **March 15, 2013**.

Please let me know if NRC staff has any questions or if this response can be sent as final.

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: 4210

Mail Envelope Properties (554210743EFE354B8D5741BEB695E6560C089D)

Subject: Advanced Response to U.S. EPR Design Certification Application RAI No. 555 (6611), FSAR Ch. 7, Question 07.01-53
Sent Date: 2/1/2013 9:02:14 PM
Received Date: 2/1/2013 9:03:59 PM
From: WILLIFORD Dennis (AREVA)

Created By: Dennis.Williford@areva.com

Recipients:
"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
"TOLLEY Tracey (AREVA)" <Tracey.Tollar@areva.com>
Tracking Status: None
"VANCE Brian (AREVA)" <Brian.Vance@areva.com>
Tracking Status: None
"WELLS Russell (AREVA)" <Russell.Wells@areva.com>
Tracking Status: None
"WILLS Tiffany (AREVA)" <Tiffany.Wills@areva.com>
Tracking Status: None
"MEACHAM Robert (AREVA)" <Robert.Meacham@areva.com>
Tracking Status: None
"Canova, Michael" <Michael.Canova@nrc.gov>
Tracking Status: None
"Snyder, Amy" <Amy.Snyder@nrc.gov>
Tracking Status: None

Post Office: FUSLYNCMX03.fdom.ad.corp

Files	**Size**	**Date & Time**	
MESSAGE	5126	2/1/2013 9:03:59 PM	
RAI 555 Advanced Response Q 07.01-53 US EPR DC.pdf			275387

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

Advanced Response to

Request for Additional Information No.555, Question 07.01-53

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 07.01-53:

OPEN ITEM

Follow Up to RAI 505, Question 07.01-48

The staff requests the applicant provide additional information on how the U.S. EPR Design takes into account and bounds the effects of potential failure(s) of the Process Automation System (PAS) and Process Information and Control Systems (PICS) on safety-related components and systems. This question is a follow-on question based on technical information presented to the staff within the applicant's response to RAI 505, Question 07.01-48.

IEEE Std. 603-1991, Clause 5.6.3.1(2), “Isolation”, as endorsed by 10 CFR 50.55a(h), states in part, that no credible failure on the non-safety side of an isolation device shall prevent any portion of a safety system from meeting its minimum performance requirements during and following any design basis event requiring that safety function. According to U.S. EPR FSAR, Tier 2, Section 7.1, Revision 3, PAS and PICS are non-safety-related systems. The PAS provides controls for both safety-related and non-safety-related equipment. The Process Information and Control System (PICS), by means of computer network connections through PAS, can provide manual, component-level and grouped control of safety-related equipment, according to FSAR Tier 2, Table 7.1-3, Sheet 1 of 2. Therefore, failures of PAS and PICS can directly affect safety-related components. U.S. EPR FSAR, Tier 2, Section 15.0.0.3.8 discusses single failures that have been incorporated into the Accident Analysis. Table 15.0-11 provides a listing of the most limiting single failure for each design basis event in the Accident Analysis. Based upon the above information and the information contained in the FSAR, it appears that PAS could fail in such a way that its failure could:

1. Potentially cause a system perturbation for which the Protection System (PS) and other safety systems may have to mitigate.

2. Potentially inhibit the ability of the PS and other safety systems to meet their performance requirements, such as those required by Clause 4 of IEEE Std. 603-1991 (Design Bases). In particular, Sub-clause 4.10 establishes the requirement for response times of the safety system. A failure(s) of PAS calls into question whether the stated response times in FSAR Table 15.0-8 for the Engineered Safety Features Actuation System (ESFAS) are adequate to protect the plant and ensure design basis limits are not exceeded in the presence of a failure of PAS or a failure of PAS concurrent with a design basis event. Potentially inhibit the ability of the PS and other safety systems to meet their performance requirements, such as those required by Clause 4 of IEEE Std. 603-1991 (Design Bases). In particular, Sub-clause 4.10 establishes the requirement for response times of the safety system. A failure of PAS calls into question whether the stated response times in FSAR Table 15.0-8 for the Engineered Safety Features Actuation System (ESFAS) are adequate to protect the plant and ensure design basis limits are not exceeded in the presence of a failure of PAS or a failure of PAS concurrent with a design basis event.

3. Exceed the bounds of the analyzed events documented in FSAR Table 15.0-11. For example, if a failure of PAS or PICS occurs, the failure could happen in such a way that it affects all four divisions of a safety-related component and not just a single division as captured in Table 15.0-11.

As identified in Clause 5.6.3.1(2) of IEEE Std. 603-1991 above, credible failures of non-safety systems must not prevent any portion of a safety system from meeting its minimum performance requirements. The staff considers a software failure of the non-safety-related PAS and PICS to be a credible failure that could potentially impact multiple safety divisions. For example, in FSAR Section 15.1.4.1, the applicant postulates, the inadvertent opening of a single Main Steam Relief Train Isolation Valve (MSRIV), concurrent with a single failure of the associated MSRCV failing open. This AOO only pertains to a single affected Steam Generator (SG). The applicant considers the single failure of the MSRCV as the most severe single failure. The analysis in FSAR Section 15.1.4.1 does not appear to be comprehensive for the full scope of possible PAS failures considering that a software error in PAS could potentially cause the inadvertent opening of a MSRIV concurrent with a failure of the MSRCV in all four SGs at the same time. It is not clear from the analysis that the plant would be adequately protected from this type of failure, or why a PAS failure of this type and magnitude is not credible. The staff has similar concerns with the other non-safety-related control system failures in the safety analysis as well..

The staff cannot determine through a review of available design documentation that a failure of PAS would not adversely impact the performance of safety-related components and safety systems such as PS or the Safety Automation System (SAS). Based upon teleconferences with the applicant and the applicant's response to RAI 505, Question 07.01-46, it is clear that the applicant has considered the effects of a PAS/PICS failure on safety-related components and/or trains of components. With Revision 3 of the FSAR, the applicant introduced the Operational I&C Disable Switch (OICS). The OICS is located on the Safety Information and Control System (SICS). The design function of the OICS is to ensure that, when the OICS is enabled, manual commands from the SICS are not overridden by automatic commands from PAS by disabling automatic commands from PAS at the priority module. In subsequent teleconferences with the applicant, the staff learned that the additional design function of the OICS is to preclude any negative system effects as a result of PAS/PICS failures. The OICS addresses PAS failures from a controls standpoint, but the applicant doesn't appear to fully evaluate the full scope of PAS failures and how they would impact the accident analysis; particularly with regards to safety I&C system performance.

The staff requests the applicant to address the following questions:

a. Demonstrate how the plant would be adequately protected from each PAS failure, including software and hardware failures that could prevent or delay the safety function in multiple safety divisions. Are the safety functions and their corresponding response times in FSAR Table 15.0-8 sufficient to protect the plant if a PICS/PAS failure occurs, and is the PS capable of mitigating a Design Basis Event (DBE) concurrent with a PICS/PAS failure?

b. If the applicant does not consider certain failures of PICS/PAS to be credible, provide justification on why those specific failures are not credible.

Response to Question 07.01-53

The response to this question is divided into three parts:

1. The treatment of postulated failure(s) of the process automation system (PAS) and process information and control systems (PICS) in the U.S. EPR FSAR Tier 2, Chapter 15–Safety Analysis, will be provided.

2. The design features of PAS are described, as well as the consequences of postulated PAS software and hardware failures that could affect multiple safety divisions.

3. The design features of PICS are described, as well as the consequences of postulated PICS software and hardware failures that could affect multiple safety divisions.

Treatment of PAS/PICS Failures in Chapter 15 Safety Analysis

In the analysis of anticipated operating occurrences (AOOs) or postulated accidents (PAs), U.S. EPR FSAR Tier 2, Section 15.0.0.3.6, describes the treatment of non-safety-related control systems as follows:

“Non-safety-related systems, including control systems, are simulated when their operation makes the response of the event more severe. In this case, it is assumed that they function as designed. Failures of the non-safety-related systems are considered only as event initiators.”

Failures of PAS/PICS are not considered as single failures after an initiating event in the analysis of U.S. EPR FSAR Tier 2, Chapter 15, AOOs and PAs.

AREVA’s treatment of non-safety-related control system failures for the U.S. EPR design is consistent with the treatment of non-safety-related control system failures at current operating nuclear plants in the U.S. This approach is derived from the fact that non-safety-related controls are in continuous operation prior to the event. Failures of these controls during normal operation are self-announcing and can be detected and corrected by operations and fixed (or the failure could cause a plant transient that requires safety system action).

PAS Design Features and Failures

PAS Design Features

AREVA’s design for PAS is derived from the design principles from NRC regulations and DI&C-ISG-04, “Highly-Integrated Control Rooms – Communications Issues (HICRc).” Those principles include:

1. Redundancy.
2. Independence.
3. Segmentation.
4. Physical Separation.
5. EMI/RFI Qualification.

6. Electrical Isolation and Separation.
7. For software, uses development processes and procedures similar to safety-related software.

The redundancy within the PAS system is shown on U.S. EPR FSAR Tier 2, Figures 7.1-11 and 7.1-12. For the PAS (Nuclear Island), there are four redundant divisions of PAS. For the PAS (Turbine Island and Balance of Plant), there are two redundant trains of PAS. It should be noted that redundancy between divisions or trains refers to hardware architecture only. Software functionality differs between divisions or trains (see discussion on segmentation). Within each division or train, two redundant control units (CUs) are provided for processing. Note that the I&C architecture figures in the U.S. FSAR design only illustrate one CU pair per division or train; however, the segmentation of control functions will dictate that each division or train will contain multiple pairs of CUs.

The independence within PAS is described in U.S. EPR FSAR Tier 2, Section 7.1.1.4.6 (see FSAR markup).

Segmentation of critical control functions within PAS is provided to eliminate cross-channel communication between redundant control functions from division to division or train to train. The principle used is to align the divisions of PAS with the mechanical trains or electrical divisions of the safety systems. For the purposes of PAS design, critical control functions are grouped into two categories:

- PAS control of safety devices – Any PAS control function that interfaces with a safety device must be segmented.
- PAS control of critical non-safety-related equipment – Selection of critical control functions for non-safety-related equipment is described further under the PAS software failures section.

AREVA's treatment of segmentation is derived from NRC guidance in DI&C-ISG-04, public meetings with the NRC related to RAI 555, Question 07.01-53, and NRC acceptance of similar segmentation strategies for non-safety-related digital control systems. Segmentation is aimed at providing sufficient diversity in the application software such that the consequences of failures are restricted to a single PAS division or train. Diversity is achieved by two key elements:

- Critical control functions can be allocated to different CU pairs to ensure that failure of a CU pair will not result in an unanalyzed condition in the U.S. EPR FSAR Tier 2, Chapter 15–Safety Analysis.
- Control functions can be allocated to CU pairs such that each CU pair contains a unique set of software. This provides sufficient diversity such that application software failures can be restricted to a single CU pair.

Specific application of this segmentation principle to PAS is discussed below in the "PAS Failures – Application Software" section.

Physical separation of divisions and trains of PAS is described in U.S. EPR FSAR Tier 2, Section 7.1.1.4.6 (see attached markup).

EMI/RFI qualification of PAS is described in U.S. EPR FSAR Tier 2, Section 7.1.1.4.6 (see attached markup).

Electrical isolation and separation of PAS is described in U.S. EPR FSAR Tier 2, Section 7.1.1.4.6 (see attached markup).

The software development processes for PAS are described in U.S. EPR FSAR Tier 2, Section 7.1.1.4.6 (see attached markup).

PAS Failures – Application Software

AREVA considers postulated application software failures in a single PAS CU pair (or processor pair) to be credible. Concurrent application software failures in multiple CU pairs are not considered credible for the following reasons.

1. Integrity of Software. The design principles listed below are used for the software design of PAS.

   a. A structured and modular architecture is applied.

   b. Operating system and application software are separated.

   c. Early detection of failures is facilitated by the self-diagnosis functions of the digital system.

   d. Operating system software is implemented in a high-level programming language. All functions execute with cyclical single task processing and no interrupts.

   e. Operating system software performs only the minimal necessary functions, such as initialization, periodic execution of required function, error handling, etc.

   f. Application software is designed in a graphically symbolized manner, using a problem oriented language, so that functions can be easily understood.

   g. For PAS and PICS, development processes and procedures are used similar to safety systems.

2. Software common cause failures (SWCCF) are systematic failures that occur when failures of separate structures, systems, and components (SSCs) are triggered concurrently. A systematic failure is related, in a deterministic way, to a certain cause. A failure will always occur when the design fault is challenged by the triggering mechanism. In order for such a failure to occur, the following conditions must be present:

   a. A systematic fault must exist in multiple components in the integrated system.

   b. A triggering event must occur to challenge the systematic fault.

   The system may contain systematic faults. However, the faults do not become failures until they are challenged; and, therefore, are not harmful. By segmenting the critical control functions between CU pairs; and by operating those pairs asynchronously, with separate sensor inputs, the simultaneous fault probability is reduced so as to not be credible.

3. Software trajectory is the execution path through the software instructions. A deterministic software trajectory does not change in response to events. Such a software trajectory executes in the following manner:

   a. Execution sequence is deterministic. There is only one software trajectory; that is, all the application code is executed every cycle. The application code and basic platform software, such as modules or function blocks used to develop applications, do not contain branches or interrupts that could cause different code than is executed normally to be executed in response to input state changes or external events. The operating system may utilize simple clock cycle interrupts to schedule multiple application and/or diagnostic tasks.

   b. Deterministic execution sequence alone cannot eliminate common cause failure (CCF). However, when combined with several of the functional diversity attributes discussed below, it limits the likelihood of software errors being triggered by external input state changes; and, therefore, limits the likelihood that these software errors could result in common cause failure. If input state change cannot alter software trajectory (i.e., order of execution) then the input state changes are unlikely to trigger CCF. Real time software execution is not utilized in any process.

   c. Resource allocation is static. Memory and I/O device allocation are established at the time the application program is compiled, assembled, and downloaded to the processor. Once the application has been downloaded, resource allocation cannot be altered. Does not manage any file systems; hence, requests to read from or write to a file system cannot alter program execution sequence.

   d. Does not implement any process interrupts. The sequence of program execution cannot be altered by events generated in the process.

   e. Operates asynchronously from other processors in redundant channels of the same or other systems.

   f. Manages and isolates network communications independently from the application. Communication activity does not affect execution sequence or timing of the application.

   These characteristics of modern digital control systems reduce the probability of multiple software failures in different processers.

4. Functional diversity can significantly lessen the likelihood that these time-dependent failures will occur concurrently in multiple processors. Therefore, functional differences can significantly lessen the likelihood of time dependent CCF. Functional diversity attributes may include, but are not limited to:

   a. Asynchronous operation.

   b. Different algorithms.

   c. Different inputs.

   d. Different outputs.

   e. Different modes.

   f. Different memory allocation.

g. Different cycle times (Redundant divisions or trains with different processor clock rate or application implementation).

h. Different boot or reset time intervals and sequence.

Application of these design principles, especially the principle of segmentation, to a modern digital system that reflects the software design as described above, results in the conclusion that the diversity of the CU pairs from division to division or train to train is sufficient to conclude that although failure of a single processor pair within a division or train is credible, failures of multiple processor pairs within a single division or train or within multiple divisions or trains are not credible.

The segmentation of control functions in the PAS CU's results in assurance that no single set of processors' software is identical to another set in another division or train. By locating non-critical software functions systematically so that processors with critical functions do not have the same non-critical functions, the processors' sets of software are not identical and sufficiently diverse from division to division. This hardware segmentation and software diversity arrangement of functions eliminates credible software common cause failures that can cause spurious actuations of multiple critical safety related components. CU pairs do not communicate with other CU pairs in the same division or between divisions. Any PAS control function that interfaces with a safety device must be segmented. The principle used is to align the divisions of PAS with the mechanical trains or electrical divisions of the safety equipment.

The U.S. EPR PAS design takes advantage of this segmentation design principle to prevent simultaneous failures of software in multiple divisions or trains of PAS. The segmentation design principle will be applied to two groups of critical control functions in PAS:

- PAS control of safety devices - Any PAS control function that interfaces with a safety device must be segmented, and
- PAS control of critical non-safety-related equipment.

To determine the population of critical non-safety-related control functions, AREVA utilized a two-step process. First, the non-safety control functions of PAS described in U.S. EPR FSAR Tier 2, Chapters 7.7.2.2.1 through 7.7.2.2.5, were reviewed to determine which functions were “critical.” For the purposes of this review, “critical” non-safety control functions were defined as a failure of which could cause a transient in the Reactor Coolant System that would require some form of automatic action or operator action to correct. Based on this definition, the following PAS non-safety control functions were defined as critical:

a. RCS Pressure Control – performed by pressurizer (PZR) heaters or spray.

b. Pressurizer Level Control – performed by control valves in located in CVCS letdown lines.

c. RCS Loop Level Control – enabled at cold shutdown conditions, controlling letdown flow rate.

d. Steam Generator Level Control – matching feedwater flow to steam demand.

e. Main Steam Pressure Control – providing overpressure control by modulating the turbine bypass valves.

Second, the non-safety control functions of PAS described in Chapter 15 of the FSAR were reviewed to determine which functions were "critical." For the purposes of this review, "critical" non-safety control functions were also defined as a failure of which could cause a transient in the Reactor Coolant System that would require some automatic action or operator action to correct. Based on this definition, the following additional PAS non-safety control function was defined as critical:

f. Feedwater Temperature – Feedwater Heater Bypass Valves

These critical control functions in PAS were then segmented by allocating functionality to different CU pairs. The functional allocation of the critical control functions is shown in the table below.

Critical Non-safety Control Function Segmentation of PAS Control Units

PAS AP Pair Division-Allocation	Function Description
PAS CU Pair 1-1	LPFWH Bypass 1
PAS CU Pair 1-2	HPFWH Bypass 1
PAS CU Pair 2-1	LPFWH Bypass 2
PAS CU Pair 2-2	HPFWH Bypass 2
PAS CU Pair 3-1	LPFWH Bypass 3
PAS CU Pair 4-1	LPFWH Bypass 4
PAS CU Pair 4-2	LPFWH Bypass 5
PAS CU Pair 1-3	MFW Flow, SG1 Level Control
PAS CU Pair 2-3	MFW Flow, SG2 Level Control
PAS CU Pair 3-2	MFW Flow, SG3 Level Control
PAS CU Pair 4-3	MFW Flow, SG4 Level Control
PAS CU Pair 1-4	Turbine Bypass Valve 1
PAS CU Pair 2-4	Turbine Bypass Valve 2
PAS CU Pair 3-3	Turbine Bypass Valve 3
PAS CU Pair 4-4	Turbine Bypass Valve 4
PAS CU Pair 1-5	Turbine Bypass Valve 5
PAS CU Pair 2-5	Turbine Bypass Valve 6
PAS CU Pair 3-4	CVCS Letdown Valve Control 1
PAS CU Pair 4-5	CVCS Letdown Valve Control 2

Segmentation of critical control functions to different CU pairs in combination with systematic assignment of non-critical control functions to CU pairs will ensure that the

software on each CU pair is unique. This software diversity ensures that concurrent software failures across PAS divisions or trains is prevented.

From a failure modes perspective, the following table lists credible failure modes for the outputs of digital control systems as a result of software defects that have been triggered to become faults:

Analog Outputs	Discrete Outputs
Fail High: Spurious actions alert operator	**Fail High: Spurious actions alert operator**
• Full scale indications	• Equipment stops
• Valves wide open	• Valves change position
• Pumps full speed	
• Heaters full output	
Fail Low: Spurious actions alert operator	**Fail Low: Spurious actions alert operator**
• Bottom scale indications	• Equipment starts
• Valves fully closed	• Valves change position
• Pumps minimum speed	
• Heaters minimum output	
Fail As-Is: No operator alerts in the short term	**Fail As-Is: No operator alerts in the short term**

Software faults that result in output state changes are immediately detectable and correctable. System misoperation, that results in outputs failing to an extreme value (high/low, open/closed), will alert the operator to the malfunction. If a pump starts when it is not expected to be running, or a valve opens when it is expected to be closed, the operator will recognize it and will take prompt corrective action. It is reasonable to judge that software faults that cause spurious actions will be recognized and corrected during development, implementation, maintenance, or operation phases of an adequate software lifecycle process.

Postulated software failures could result in one of three scenarios: (1) processor lock up where the processor stops cycling and gives no outputs (for a valve, it stops in place), (2) processor lockup where the outputs drive the control elements to the minimum state (for a valve, drive it closed), and (3) processor failure where the outputs drive control elements to a maximum state (for a valve, drive it open). Given these failure states, the consequences of a postulated software failure on each of the critical control functions is as follows:

1. RCS Pressure Control – The control elements for this function are pressurizer heaters and spray valves. Any of the three failures mentioned above will cause a slow transient of the RCS pressure either up or down. This transient will reach alarm points so that the operator will recognize the failure and can take corrective action. If the operator action fails to make the correction before the RCS pressure limitation setpoint is reached, these limitation functions will take an appropriate action to control the sprays or heaters. This limitation

function will be allocated to another PAS CU pair. No further analysis of this failure and the accompanying transient is necessary.

2. Pressurizer Level Control – The control elements for this function are the control valves located in the CVCS letdown lines. The initial conditions for this event are that one CVCS pump and one letdown valve are operating. Any of the three failures mentioned above will cause a slow transient of pressurizer level up or down. This transient will reach an alarm setpoint so that the operator will recognize the failure and can take corrective action.

   - One of these postulated transients is analyzed in U.S. EPR FSAR Tier 2, Chapter 15, Section 15.5.2, "CVCS Malfunction that Increases Reactor Coolant Inventory." This analysis makes the conservative assumption that two CVCS charging pumps actuate and letdown is isolated. This is the most conservative assumption for increasing the RCS inventory, but it exceeds the normal PAS operating configuration. The transient is isolated by a reactor trip. Since the pressurizer level control is segmented between PAS CU Pairs 3-4 and 4-5, and the analyzed failure bounds a credible PAS failure of a single processor segment, no further analysis of this failure and accompanying transient is necessary.
   - Failure of control valves in place will cause a slow-moving transient in pressurizer level that the operator can recognize and correct.
   - Failure of control valves wide open is bounded by a small break LOCA (break in nozzle of pipe), which is analyzed in U.S. EPR FSAR Tier 2, Chapter 15, Section 15.6.5, "Loss of Coolant Accidents Resulting from Spectrum of Postulated Piping Breaks within the Reactor Coolant Pressure Boundary." No further analysis of this transient is necessary.

3. RCS Loop Level Control – This control function is used in Mode 5 and 6. Letdown flow rate is again used as the controlled variable for positioning of the letdown control valves. Failure of a control valve, while it is being used in this mode, will result in RCS loop level either increasing or decreasing to the alarm setpoints, at which time the operator will take the appropriate action to assure that the core continues to be covered and that no boiling occurs in the RCS primary coolant. In the event that the hot leg level goes low enough to trip the RHR pumps for equipment protection, safety logic in the PS will initiate the MHSI pumps to protect the core (see U.S. EPR FSAR Tier 2, Figure 7.3.2). No further analysis of this transient is required.

4. Steam Generator Level Control – The control elements used to match feedwater flow to steam demand are the feedwater (FW) control valves. Control of full-load FW control valves are segmented as follows: MFW for SG-1–Pair 1-3, MFW for SG-2–Pair 2-3, MFW for SG3–Pair 3-2, and MFW for SG4–Pair 4-3.

   - For a failure of one main feedwater (MFW) control valve as is, depending on the steam demand when the failure occurs, a slow moving steam generator level would occur potentially leading to an overheating or overcooling transient. These transients are bounded by wide-open or fully-closed MFW valve scenarios that are analyzed in U.S. EPR FSAR Tier 2, Chapter 15.
   - For a failure of the control valves wide open, an increase in heat removal by the secondary system transient is analyzed in U.S. EPR FSAR Tier 2, Chapter 15, Section 15.1.2. No further analysis of these transients is required.

- For failure of a feedwater control valve closed, a loss of normal feedwater flow from main feedwater sources is analyzed in U.S. EPR FSAR Tier 2, Chapter 15, Section 15.2.7. No further analysis of these transients is required.

5. Main Steam (MS) Pressure Control – The purpose of the MS pressure control function is to provide MS overpressure control and limitation in case of load reduction due to load steps, load ramps, or load rejection. MS pressure is controlled by automatically modulating the turbine bypass valves. Control of the turbine bypass valves is segmented as follows: TBV1–Pair 1-4, TBV2–Pair 2-4, TBV3–Pair 3-3, TBV4–Pair 4-4, TBV5–Pair 1-5, and TBV6-Pair 2-5.

   These valves are closed during normal operation.

   - A failure of the control function that calls for a demand to be closed would not change the valve position.
   - A failure that locks up the output during normal operation also will not change the valve position.
   - A failure that opens these turbine bypass valves is analyzed in U.S. EPR FSAR Tier 2, Chapter 15, Section 15.1.3, “Increase in Steam Flow.” No further analyses of these transients are required.

6. Feedwater Temperature – The feedwater heater bypass valves are supplied in the event that a feedwater heater develops a tube leak and must be isolated. The bypass valves are normally closed, and the feedwater temperature is controlled by the level of condensate in the shell of each feedwater heater. Control of the feedwater heater bypass valves is segmented as follows: LPFWH Bypass 1–Pair 1-1, HPFWH Bypass 1–Pair 1-2, LPFWH Bypass 2–Pair 2-1, HPFWH Bypass 2–Pair 2-2, LPFWH Bypass 3–Pair 3-1, LPFWH Bypass 4–Pair 4-1, and LPFWH Bypass 5, Pair 4-2.

   - A control system failure that would close a bypass valve would have no impact since the valves are normally closed.
   - A control system failure that would open a bypass valve is analyzed in U.S. EPR FSAR Tier 2, Chapter 15, Section 15.1.1, “Decrease in Feedwater Temperature.” Only one bypass valve is assumed to fail open as control for all these valves is segmented. No further analysis is required.

   Therefore, it is unlikely that a software defect that results in output state changes: (1) will affect multiple processors (within a division/train or between divisions/trains), and (2) will ever become a source of a SWCCF. Further, should a software defect result in output state changes, then the effects will be bounded by the existing U.S. EPR FSAR Tier 2, Chapter 15–Safety Analysis.

PAS Failures – Operating System Software

The PAS platform for the U.S. EPR plant is not specified to date. Therefore, no specific features can be discussed in response to this question. However, in general, should the operating system software fail, the application software would stop operating and the failure consequences would be the same as discussed above. The arguments presented for reducing the probability of a SWCCF for the application software can also apply to the operating system,

and AREVA's position on this issue is that this type of failure is not credible in a manner that would affect CU pairs in multiple divisions or trains.

PAS Failures – Hardware Failures

From a hardware perspective, failures of PAS can be broadly grouped into five categories. The failures and resultant consequences are summarized as follows:

- Failure of a PAS Division or Train – A complete failure of the PAS hardware in a division or train is considered incredible. The most significant credible PAS hardware failure is a failure of a PAS communications processor (see discussion below). This event requires no further analysis.
- Failure of a PAS Communications Processor – Due to the segmentation of control functions, a failure of either a communications processor or communication path would impact at most one division or train. The remaining 3 divisions or 1 train would continue to operate normally to accomplish their functions. Since the control valves being controlled by PAS would fail as-is upon loss of the control signal (i.e., communication failure), the plant would not go into a transient. That is, normally open/closed valves would remain in their current state (e.g., feedwater heater bypass valves and turbine bypass valves would remain closed) and control valves would fail as-is (e.g., MFW control valves and Letdown control valves would remain in a fixed, pre-failure position). The Operator would receive an alarm following the loss of control signal, and would either have the PAS communication problem repaired or would locally operate the affected control valves until the problem could be repaired.
- Loss of Power to a PAS Division or a Train – The complete failure of a PAS division or train due to a power failure is an unlikely event. This failure is discussed in U.S. EPR FSAR Tier 2, Section 7.7.2.7:

  > "PAS is powered by a battery backed source. The secondary power source is from a separate battery backed source fed from a different power bus. Upon loss of primary power to PAS, the secondary power source automatically and without interruption, maintains power. In case of a total loss of power to the plant, the battery source continued operation of the plant controls for a two hour period."

  In the unlikely event that a PAS division or train loses power, the consequences would be bounded by the failure of a PAS division or train. This event requires no further analysis.
- Failure of a PAS CU Pair – This failure is similar in consequence to a software failure as analyzed above. No further analysis is required.
- Failure of an Individual PAS CU – The failure of an individual CU would result in the redundant processor within the division or train taking over the control functions of the failed processor. No failure impact.

PICS Design Features and Failures

PICS Design Features

AREVA's design for PICS is derived from the design principles from NRC regulations and DI&C-ISG-04, "Highly-Integrated Control Rooms – Communications Issues (HICRc)." Those principles include:

1. Two operator actions where appropriate.
2. Redundancy.
3. Independence.
4. EMI/RFI Qualification.
5. Electrical Isolation and Separation.
6. For software, uses development processes and procedures similar to safety related software.

A description of these design principles have been added to U.S. EPR FSAR Tier 2, Section 7.1.1.3.2.

In the U.S. EPR design, PICS is capable of performing self-diagnostics and displaying self-diagnostic data of PAS, and other plant I&C systems, to the operators. The PICS provides robustness and reliability by utilizing redundant processing and server units. Components, implemented as part of PICS, provide physical and functional redundancy. Physical separation of redundant components into different rooms and different fire zones ensures independence of redundant divisions of PICS. The LAN system provides single failure tolerance against media interruption or failure of an active LAN component. In addition, those redundant components have redundant support systems (e.g., power supply system, etc.). Independence of the PICS is achieved through electrical and functional isolation and physical separation, as described in the following U.S. EPR FSAR Tier 2 sections and the attached markups:

- U.S. EPR FSAR Tier 2, Section 7.1.1.3.2 describes the Physical Separation of PICS.
- U.S. EPR FSAR Tier 2, Section 7.1.1.3.2 describes the EMI/RFI Qualification of PICS.
- U.S. EPR FSAR Tier 2, Section 7.1.1.3.2 describes the Electrical Isolation and Separation of PICS.

Operators initiate signals from PICS through PAS for control of safety and non-safety devices. Operation of plant components is performed through operating control windows (faceplates) on the PICS operator workstations (OWS) using a multi-step process. A single mouse click on a component icon opens the component's operational control window. This operational control window contains virtual command buttons that must be selected and clicked. This control scheme is to prevent inadvertent actuation of a function or component by single operator action. The operating control windows for modulating controls have pairs of buttons that send single pulse control commands in the desired direction with each click. An inadvertent action can only send out a single pulse command which results in a single component response.

PICS control functions are as follows to cope with potential failures of the PICS on safety-related components and systems:

- PICS may use grouped commands for all non-critical, non-safety related control functions.
- Manual grouped commands from PICS will be sent to the PAS. The segmentation scheme for PAS, as described above will preclude the unwanted actuation of components in multiple divisions or trains.
- For manual commands involving safety-related equipment, PICS will not have grouped commands that actuate components in more than one train or division at a time; manual

grouped commands for safety-related components may only be grouped within one train or division. This prevents a single failure from spuriously actuating multiple safety trains (e.g., open all four MSRTs) and, therefore, maintains the system design within the bounds of the U.S. EPR FSAR Tier 2, Chapter 15 Safety Analysis.

PICS Failures – Software Failures

The U.S. EPR design considers postulated application software failures in a single PICS server unit (SU) to be credible. Concurrent application software failures in multiple SU or software failures resulting in inadvertently operating safety-related components in multiple divisions or trains are not considered credible. No grouped commands for the manual actuation of safety-related equipment in multiple trains or divisions will be implemented in the PICS.

Spurious signals resulting from software failures affecting multiple trains or divisions, originated in the PICS, will be sent to the PAS. The U.S. EPR PICS design takes advantage of the PAS segmentation design principle to prevent simultaneous failures propagating to multiple divisions or trains of PAS.

Software faults that result in output state changes are immediately detectable and correctable. System mis-operation that results in outputs failing to an extreme value (high/low, open/closed) will alert the operator to the malfunction. If a pump starts when it is not expected to be running, or a valve opens when it is expected to be closed, the operator will recognize it and will take prompt corrective action. It is reasonable to judge that software faults that cause spurious actions will be recognized and corrected during development, implementation, maintenance, or operation phases of an adequate software lifecycle process.

PICS Software Failures – Server Unit (SU)

A failure of the application software or operation system installed on the currently active SUs is detected by the means of self-diagnosis. SU operate in a hot/master standby mode. Upon detection of a software failure, operation will be seamlessly switched over to another SU.

PICS Software Failures – Operating Terminals (OT)

The operating system for the operating terminals (OT) is used to provide graphics and data to the operator workstations. The data is provided by the SU. A failure of the OT operating system may result in partial of full loss or one or more operator workstations but will not disrupt the operation of the SU or other OTs.

PICS Failures – Hardware Failures

Complete failure of the PICS is unlikely. PICS is a highly reliable system utilizing multiple SU for operation and a redundant network bus system. PICS is also backed-up from the UPS 12-hour batteries and the station blackout diesel generators.

PICS is in a non-critical failure configuration if one component of the PICS has failed. In the event of a single component failure, sufficient redundancy still exists to permit a redistribution of tasks and computing functionality to continue utilization of the PICS to control and monitor the plant. In case of a failure of a component of the processing structures redistribution of the process resources or interface resources is performed automatically by the PICS (through

redundant mechanisms, for instance). PICS structures and components are not affected by such a failure. The operator can use the PICS as usual and the failure will not propagate to PAS.

Possible hardware failures for the PICS are:

1. Failure of a Server Unit (SU) - SU operate in a hot/master standby mode. In case of a failure of a SU a redundant SU will be used to continue uninterrupted operation of PICS.

2. Failure of an Operating Terminal (OT) - A failure of an operating terminal (OT) will result in the loss of one or more operator work stations (OWS) but will not produce erroneous signals which can be further processed by the SU and passed on to the PAS. The main purpose of the OT is to provide information and operation data to the OWS and short term storage of process data.

3. Failure of a Network Component or Gateway - The PICS network is redundant. In the event a component or gateway of the PICS network fails the redundant component is used to continue uninterrupted operation.

4. Failure of the PICS Electrical Power Supply - PICS is powered by redundant uninterruptible power supplies. The failure of one uninterruptible power supply will result in the loss of SUs, operating terminals and operator work stations associated with this power supply. PICS components associated with the redundant uninterruptible power supply will continue to be operable.

The ITAAC for electrical isolation, physical separation, and one-way communication between Class 1E and non-Class 1E equipment are in the Class 1E sections.

FSAR Impact:

U.S. EPR FSAR Tier 1, Section 2.4.9 and 2.4.10, will be added as described in the response and indicated on the enclosed markup.

U.S, EPR FSAR Tier 2, Sections 7.1.1.3.2, 7.1.1.4.6, and 7.7.2.7, will be changed as described in the response and indicated in the enclosed markup.

U.S. EPR Final Safety Analysis Report Markups

2.4.9 Process Automation System

~~There are no Tier 1 entries for this system.~~

Design Description

1.0 System Description

The process automation system (PAS) is organized into four redundant, independent divisions located in separate Safeguard Buildings. The PAS is implemented with an industrial I&C platform. It provides monitoring and control of plant systems. The PAS is non-safety related.

2.0 Arrangement

2.1 The location of the PAS equipment is as listed in Table 2.4.9-1—Process Automating System Equipment.

3.0 I&C Design Features, Displays, and Controls

3.1 Critical control functions are segmented in the PAS control units (CU).

3.2 The PAS design is accomplished through a phased approach which includes the following (or equivalent) phases:

1. System Requirements Phase.
2. System Design Phase.
3. Software/Hardware Requirements Phase.
4. Software/Hardware Design Phase.
5. Software/Hardware Implementation Phase.
6. Software/Hardware Validation Phase.
7. System Integration Phase.
8. System Validation Phase.

3.3 PAS equipment listed in Table 2.4.9-1 can function when subjected to electromagnetic interference (EMI) and radio-frequency interference (RFI).

Inspections, Tests, Analyses, and Acceptance Criteria

Table 2.4.9-2 lists the PAS ITAAC.

Table 2.4.9-1—Process Automation System Equipment

Description	Location
PAS Cabinets Division 1	Safeguard Building 1
PAS Cabinets Division 2	Safeguard Building 2
PAS Cabinets Division 3	Safeguard Building 3
PAS Cabinets Division 4	Safeguard Building 4

Table 2.4.9-2—Process Automation System ITAAC
Sheet 1 of 2

	Commitment Wording	Inspections, Tests, Analyses	Acceptance Criteria
2.1	The location of the PAS equipment is as listed in Table 2.4.9-1.	An inspection of the location of the as-built PAS equipment will be performed.	The PAS equipment listed in Table 2.4.9-1 is located as listed in Table 2.4.9-1.
3.1	Critical control functions are segmented in the PAS CUs.	An analyses will be performed to verify that non-critical control functions will be systematically located so that PAS CUs with redundant critical control functions do not have redundant non-critical control functions.	A report concludes that non-critical control functions are systematically located so that PAS CUs with redundant critical control functions do not have redundant non-critical control functions.
3.2	The PAS design is accomplished through a phased approach which includes the following (or equivalent) phases: 1) System Requirements Phase. 2) System Design Phase. 3) Software/Hardware Requirements Phase. 4) Software/Hardware Design Phase. 5) Software/Hardware Implementation Phase. 6) Software/Hardware Validation Phase. 7) System Integration Phase. 8) System Validation Phase.	a. Analyses will be performed to verify that the outputs for the PAS requirements phase conform to the requirements of that phase. b. Analyses will be performed to verify that the outputs for the PAS design phase conform to the requirements of that phase. c. Analyses will be performed to verify that the outputs for the PAS software/hardware requirements phase conform to the requirements of that phase.	a. A report concludes that the outputs for the PAS requirements phase conform to the requirements of that phase. b. A report concludes that the outputs for the PAS design phase conform to the requirements of that phase. c. A report concludes that the outputs for the PAS software/hardware requirements phase conform to the requirements of that phase.

Table 2.4.9-2—Process Automation System ITAAC
Sheet 2 of 2

Commitment Wording		Inspections, Tests, Analyses	Acceptance Criteria
		d. Analyses will be performed to verify that the outputs for the PAS software/hardware design phase conform to the requirements of that phase.	d. A report concludes that the outputs for the PAS software/hardware design phase conform to the requirements of that phase.
		e. Analyses will be performed to verify that the outputs for the PAS software/hardware implementation phase conform to the requirements of that phase.	e. A report concludes that the outputs for the PAS software/hardware implementation phase conform to the requirements of that phase.
		f. Analyses will be performed to verify that the outputs for the PAS software/hardware validation phase conform to the requirements of that phase.	f. A report concludes that the outputs for the PAS software/hardware validation phase conform to the requirements of that phase.
		g. Analyses will be performed to verify that the outputs for the PAS integration phase conform to the requirements of that phase.	g. A report concludes that the outputs for the PAS integration phase conform to the requirements of that phase.
		h. Analyses will be performed to verify that the outputs for the PAS validation phase conform to the requirements of that phase.	h. A report concludes that the outputs for the PAS validation phase conform to the requirements of that phase.
3.3	PAS equipment listed in Table 2.4.9-1 can function when subjected to EMI and RFI.	Type tests or type tests and analyses will be performed to demonstrate that the PAS equipment listed in Table 2.4.9-1 can function when subjected to EMI and RFI.	PAS equipment listed in Table 2.4.9-1 can function when subjected to EMI and RFI.

2.4.10 Process Information and Control System

Design Description

1.0 System Description

The process information and control system (PICS) is organized into two redundant, independent divisions located in separate Safeguard Buildings. The ~~process information and control system (~~PICS~~)~~ is implemented with an industrial I&C platform. It provides monitoring and control of plant systems. The PICS is non-safety related and is provided in both the main control room (MCR) and the remote shutdown station (RSS).

2.0 Arrangement

2.1 The location of the PICS equipment is as listed in Table 2.4.10-1—Process Information and Control System Equipment.

3.0 I&C Design Features, Displays, and Controls

3.1 Deleted.

3.2 The PICS design is accomplished through a phased approach which includes the following (or equivalent) phases:

1. System Requirements Phase.
2. System Design Phase.
3. Software/Hardware Requirements Phase.
4. Software/Hardware Design Phase.
5. Software/Hardware Implementation Phase.
6. Software/Hardware Validation Phase.
7. System Integration Phase.
8. System Validation Phase.

3.3 Deleted.

3.4 Electrical isolation is provided on PICS connections between the RSS and the MCR to prevent the propagation of credible electrical faults.

3.5 The capability to transfer control of the PICS from the MCR to the RSS exists in a fire area separate from the MCR and allows transfer of control without entry into the MCR.

3.6 PICS equipment listed in Table 2.4.10-1 can function when subjected to electromagnetic interference (EMI) and radio-frequency interference (RFI).

3.7 Manual grouped commands on PICS are segmented such that one command cannot send signals to multiple segmented process automation system (PAS) Control Units (CU) which control critical PAS functions.

Inspections, Tests, Analyses, and Acceptance Criteria

Table 2.4.10-2~~1~~ lists the PICS ITAAC.

Table 2.4.10-1—Process Information and Control System Equipment

Description	Location
PICS Cabinets Division 1	Safeguard Building 2
PICS Cabinets Division 2	Safeguard Building 3

Table 2.4.10-2—Process Information and Control System ITAAC
Sheet 1 of 3

	Commitment Wording	Inspections, Tests, Analyses	Acceptance Criteria
2.1	The location of the PICS equipment is as listed in Table 2.4.10-1.	An inspection of the location of the as-built PICS equipment will be performed.	The PICS equipment listed in Table 2.4.10-1 is located as listed in Table 2.4.10-1.
3.1	Deleted.	Deleted.	Deleted.
3.2	The PICS design is accomplished through a phased approach which includes the following (or equivalent) phases: 1) System Requirements Phase. 2) System Design Phase. 3) Software/Hardware Requirements Phase. 4) Software/Hardware Design Phase. 5) Software/Hardware Implementation Phase. 6) Software/Hardware Validation Phase. 7) System Integration Phase. 8) System Validation Phase.	a. Analyses will be performed to verify that the outputs for the PICS requirements phase conform to the requirements of that phase. b. Analyses will be performed to verify that the outputs for the PICS design phase conform to the requirements of that phase. c. Analyses will be performed to verify that the outputs for the PICS software/hardware requirements phase conform to the requirements of that phase. d. Analyses will be performed to verify that the outputs for the PICS software/hardware design phase conform to the requirements of that phase.	a. A report concludes that the outputs for the PICS requirements phase conform to the requirements of that phase. b. A report concludes that the outputs for the PICS design phase conform to the requirements of that phase. c. A report concludes that the outputs for the PICS software/hardware requirements phase conform to the requirements of that phase. d. A report concludes that the outputs for the PICS software/hardware design phase conform to the requirements of that phase.

Table 2.4.10-2—Process Information and Control System ITAAC
Sheet 2 of 3

Commitment Wording		Inspections, Tests, Analyses	Acceptance Criteria
		e.Analyses will be performed to verify that the outputs for the PICS software/hardware implementation phase conform to the requirements of that phase.	e. A report concludes that the outputs for the PICS software/hardware implementation phase conform to the requirements of that phase.
		f.Analyses will be performed to verify that the outputs for the PICS software/hardware validation phase conform to the requirements of that phase.	f. A report concludes that the outputs for the PICS software/hardware validation phase conform to the requirements of that phase.
		g.Analyses will be performed to verify that the outputs for the PICS integration phase conform to the requirements of that phase.	g. A report concludes that the outputs for the PICS integration phase conform to the requirements of that phase.
		h.Analyses will be performed to verify that the outputs for the PICS validation phase conform to the requirements of that phase.	h. A report concludes that the outputs for the PICS validation phase conform to the requirements of that phase.
3.3	Deleted.	Deleted.	Deleted.
3.4	Electrical isolation is provided on PICS connections between the RSS and the MCR to prevent the propagation of credible electrical faults.	a. Type tests, analyses, or a combination of type tests and analyses will be performed on the electrical isolation devices between PICS connections between the RSS and the MCR.	a. A report concludes that the Class 1E isolation devices used between PICS connections between the RSS and the MCR prevent the propagation of credible electrical faults.
		b. An inspection will be performed on connections between the as-built RSS and the as-built MCR.	b. Class 1E electrical isolation devices exist on connections between the RSS and the MCR.

Table 2.4.10-2—Process Information and Control System ITAAC
Sheet 3 of 3

Commitment Wording		Inspections, Tests, Analyses	Acceptance Criteria
3.5	The capability to transfer control of the PICS from the MCR to the RSS exists in a fire area separate from the MCR and allows transfer of control without entry into the MCR.	a. An inspection will be performed to verify that as-built controls exist in a fire area separate from the MCR for transfer of control of the PICS from the MCR to the RSS. b. Tests will be performed to verify that controls allow transfer of control of the PICS from the MCR to the RSS without entry into the MCR.	a. Controls exist in a fire area separate from the MCR for transfer of control of the PICS from the MCR to the RSS. b. Transfer switches perform transfer of control of the PICS from the MCR to the RSS without entry into the MCR.
3.6	PICS equipment listed in Table 2.4.10-1 can function when subjected to EMI and RFI.	Type tests or type tests and analyses will be performed to demonstrate that the PICS equipment listed in Table 2.4.10-1 can function when subjected to EMI and RFI.	PICS equipment listed in Table 2.4.10-1 can function when subjected to EMI and RFI.
3.7	Manual grouped commands on PICS will be segmented such that one command cannot send signals to multiple segmented PAS CUs which control critical PAS functions.	An analysis will be performed to demonstrate that manual grouped command signals from PICS are not sent to multiple segmented PAS CUs which control critical PAS functions.	A report concludes that manual grouped command signals from PICS are not sent to multiple segmented PAS CUs which control critical PAS functions.

the RSS. Monitoring-only capabilities are provided in the technical support center (TSC) for support of emergency response operations.]*

Classification

[*The PICS is classified as non-safety-related, supplemented grade (NS-AQ).*]*

Functions

Table 7.1-3 shows the functions of the PICS.

Interfaces

Table 7.1-4 shows the interfaces of the PICS.

Architecture

Figure 7.1-2 shows the basic architecture of the PICS.

The PICS consists of gateways, servers, operator workstations, plant overview panels (POP), and firewalls.

Redundancy

The PICS is designed such that a single failure will not prevent the system from performing any of its functions. Overall system redundancy is achieved through the following means:

- Redundancy in Plant Systems - The plant automation systems, with which the PICS interfaces, are designed to continue to operate automatically upon a loss of a PICS signal.
- Divisional Redundancy - The PICS equipment is strategically divided between the Safeguards Building divisions 2 and 3. If a loss of some of the operator terminal screens occurs, the hardware arrangement prevents a total loss of PICS.
- Control Redundancy - Multiple PICS workstations are located in the MCR. Each workstation has the capability of controlling every function or component capable of being controlled by the PICS system. In the event of the loss of a PICS workstation, control of the systems, functions, and components can be accomplished from another PICS workstation within the MCR.

Redundant gateways are provided for unidirectional communication with the PS, safety automation system (SAS), bidirectional communication with process automation system (PAS), reactor control, surveillance and limitation (RCSL), and TG I&C. The PICS receives unidirectional signals from the PS and SAS to receive status information on those systems. The PICS communicates bi-directionally with the RCSL and TG I&C for control of reactivity control systems and the TG, respectively.

Independence

The PICS is designed such that there is independence between the PICS and any safety-related systems or functions. A failure of the PICS shall not prevent any of the safety-related systems from performing their functions.

The following principles are utilized to ensure independence:

- One-way communication between safety-related and non-safety-related systems.
- Electrical isolation.
- Geographic (physical) separation.

Servers are provided for data exchange between the automation bus and the HMI bus. The servers perform functions such as data message validation, short term data storage, and alarm management. Redundant servers are provided so that the PICS remains operational in case of a failure of a single server. Multiple sets of redundant servers may be used to subdivide functionality (e.g., control and indication, alarm, historian, etc).

PICS workstations with control and monitoring capabilities are located in the MCR and RSS. Normally, the operator displays in the RSS are in supervisory mode (view only) to prevent plant control until authorized in accordance with plant procedures. Operator displays are provided in the TSC with monitoring only capabilities to assist in plant emergency response.

The number of terminals per workstation, and number and location of the operator workstations is determined as a result of the human factors design process described in Chapter 18.

Plant overview panels are provided in the MCR, and other locations such as the TSC as desired. These are wide screen displays that are capable of providing continuously visible information to the operator.

Redundant firewalls are provided for unidirectional transfer of information from the PICS to plant business networks. Remote access to the PICS is not possible.

The PICS may include other functional units as necessary to carry out its functions. Examples are:

- Long term data storage units.
- Networked printers.
- Service equipment.

Equipment

The PICS is implemented with an industrial I&C platform.

The servers consist of industrial computers. Operator workstations typically consist of computers, displays, and input devices (i.e., computer mice and keyboards). The operator may use several monitors that share input devices. These monitors display different plant functions, and the display content is interchangeable. The POP is a set of large panels that display an overview of plant and system status. Equipment such as network switches and electrical and fiber optic cable are provided to support data communications. The PICS equipment is capable of trending of information to provide situational awareness by the operator. In addition, the PICS has recording capability so that historical data can be recalled by the operator.

The plant annunciator is integrated into the PICS operating and monitoring system. Special screens display and organize alarms and warnings based on their status and relative level of importance. An alarm hierarchy with a color coding system is used to immediately alert the operator of the importance of the alarm based on the relevance to plant safety.

The PICS is used to control both safety-related (via the process automation system (PAS) and the priority and actuator control system (PACS)) and non-safety-related process systems. The PICS implements these measures to preclude spurious actuation of plant equipment:

- Operation of plant equipment is performed using a two-step process. A single mouse click on a component is followed by a verification step requiring a second single mouse click, so a single inadvertent action by the operator does not result in a command signal.

- Touch screen displays are not used.

Qualification Requirements

[*The PICS is intended to be used during normal, accident, and severe accident conditions as long as it is available. The PICS equipment is located in Safeguard Buildings that provide a mild environment during and following design basis events (DBE). Equipment selected for use in the PICS will be rated by the manufacturer to operate under the mild environmental conditions expected to exist at its location during the events that the equipment is expected to be used.*]*

EMI/RFI

The equipment used in the PICS is evaluated for EMI/RFI performance using the principles described in RG 1.180. Strict compliance with these requirements is not required; however, the following shall be demonstrated:

- The electromagnetic emissions from this equipment is sufficiently low so that safety-related equipment in proximity is not adversely affected.

- The electromagnetic susceptibility of this equipment is adequate so that emissions from other equipment do not cause adverse effects within the system.

Examples of adverse effects include: spurious actuation of plant components that results in an undesirable plant transient, large electrical surges that can damage equipment and other adjacent equipment, or corruption of data that can result in confusing indications to the operator.

Quality Requirements

[*In its role as the primary operator interface, the PICS is required to be of supplemented quality to perform its functions in a reliable manner. The PICS is designed using a robust engineering process with appropriate reviews, verifications, tests, and approvals. Supplemented quality is achieved in the design of the PICS through the following measures:*

- *The PICS is designed, fabricated, erected, and tested under the quality assurance program described in ANP-10266A, Addendum A (Reference 42). This quality assurance program is consistent with the guidance of Generic Letter 85-06 (Reference 43).*]*

- The design of the PICS is accomplished through a phased approach, including the following (or equivalent) phases:
  - System requirements phase.
  - System design phase.
  - Software/hardware requirements phase.
  - Software/hardware design phase.
  - Software/hardware implementation phase.
  - Software/hardware validation phase.
  - System integration phase.
  - System validation phase.

- A criticality analysis is performed for the PICS software in accordance with accepted industrial practice.

- V&V of the PICS software is performed according to a V&V plan that is consistent with accepted industrial practice.

7.1.1.4.6 Process Automation System

The PAS is the main automation and control system for the plant. The PAS provides controls for both safety-related and non-safety-related equipment.

Classification

The PAS is classified as non-safety-related.

Functions

Table 7.1-3 shows the functions of the PAS.

Interfaces

Table 7.1-4 shows the interfaces of the PAS.

Architecture

Figure 7.1-11—Process Automation System Architecture (Nuclear Island) provides a functional representation of the PAS in the Nuclear Island (NI). Figure 7.1-12—Process Automation System Architecture (Turbine Island and Balance of Plant) provides a functional representation of the PAS in the Turbine Island and Balance of Plant. These figures show the redundancy within the design of PAS.

Redundancy

The PAS contains sufficient redundancy to prevent a single failure in the following conditions:

- Loss of power to the system, subsystem, or component including main processors, communication modules, network modules, I/O modules and I/O.
- Loss of a single PAS CU.
- Loss or failure of the communications path to the PICS or SICS interfaces.
- Control Unit modules are redundant.
- Based on detailed design, select field sensors are redundant.

All redundant PAS system components are maintainable during normal plant operation and can be replaced during operation. All automation processors, contained within a CU, are provided as two-fold redundant as well as the connections to the plant and terminal busses and connection to the function modules. The redundant structure operates in a hot stand-by mode. Two automation processors run in parallel and process the same inputs. If the processor in operation fails, the hot stand-by takes over operation in a transparent manner. A network from each automation processor is

connected to the function module. The use of multiple field sensors is evaluated on a case by case basis to minimize single point of failure to important control or monitoring functions. In the case of redundant field sensors, the I/O modules receive signals from each individual sensor in a non-redundant manner. The voting function is performed as part of the application program.

The PAS is comprised of four divisions located in the NI in the following buildings:

- Safeguard Buildings.
- Emergency Power Generating Buildings.
- Essential Service Water Pump Buildings.
- Nuclear Auxiliary Building (Division 4 only).
- Radioactive Waste Building (Division 4 only).

In addition, the PAS includes two trains that are located in the Turbine Island and Balance of Plant in the following buildings:

- Switchgear Buildings.
- Circulating Water Cooling Tower Structure.
- Location of different PAS divisions or trains in physically separate buildings provides physical separation of redundant functions.

The PAS implements redundant CUs within a division or train to perform its functions. The number of redundant CUs is dependent on the sizing and segmentation of the PAS. The CUs acquire hardwired signals from the SCDS, diverse actuation system (DAS), PS, SAS, RCSL, sensors, or black boxes. Outputs are sent to non-safety-related actuators directly or to the PACS. Interfaces are also provided to the TG I&C for TG operation. The CUs interface with the PICS for manual commands and display of information. CUs in the NI may utilize networked data communications between divisions to accomplish functions that require information from different divisions.

Independence

Physical independence is achieved by location of the PAS systems in different buildings and by electrical isolation.

Where the PAS interfaces with safety systems, electrical isolation through PACS, as well as physical separation, is implemented to maintain independence between the systems.

Exchanges of data between PAS and other systems are electrically isolated either by employing fiber optics connections or by implementing decoupling measures.

Equipment

The PAS is implemented with an industrial I&C platform.

The PAS generally consists of subracks, I/O modules, function processors, communication modules, and optical link modules. Fiber optic and copper cable is used for the various data and hardwired connections. Specialized components may be used.

Segmentation

The segmentation of control functions in the PAS CU's results in assurance that no single set of processors' software is identical to another set in another division or train. By locating non-critical software functions systematically so that processors with critical functions do not have the same non-critical functions, the processors' sets of software are not identical and sufficiently diverse from division to division. This hardware segmentation and software diversity arrangement of functions eliminates credible software common cause failures that can cause spurious actuations of multiple critical safety-related components. CU pairs do not communicate with other CU pairs in the same division or between divisions. Any PAS control function that interfaces with a safety device must be segmented. The principle used is to align the divisions of PAS with the mechanical trains or electrical divisions of the safety equipment.

By locating non-critical software functions systematically so that processors with critical functions do not have the same non-critical functions, the processors' sets of software are not identical and sufficiently diverse from division to division. This hardware segmentation and software diversity arrangement of functions eliminates credible software common cause failures that can cause spurious actuations of multiple critical safety related components. CU's do not communicate with other CU's in the same division or between divisions. Any PAS control function that interfaces with a safety device must be segmented. The principle used is to align the divisions of PAS with the mechanical trains or electrical trains of the safety equipment.

The AREVA PAS design takes advantage of this segmentation design principle to prevent simultaneous failures of software in multiple divisions or trains of PAS. The segmentation design principle will be applied to two groups of critical control functions in PAS:

- PAS control of safety devices - Any PAS control function that interfaces with a safety device must be segmented, and
- PAS control of critical non-safety-related equipment.

Qualification Requirements

EMI/RFI Requirements

The PAS cabinets contain all electronic equipment associated with the system. Proper grounding and limitation of the effects of EMI and RFI are essential for the functionality of PAS electronics components and are maintained by the cabinets. The design of the PAS takes into account the requirements of IEC 61000-3, IEC 61000-4, IEC 61000-6 for limits for electromagnetic compatibility, electromagnetic compatibility testing, and electromagnetic standards. However, strict compliance with this requirement is not required.~~There are no qualification requirements for the PAS equipment.~~

Quality Requirements

For the PAS equipment, the quality requirements will be consistent with the Quality Assurance Plan for non-safety-related equipment as described in Addendum A of ANP-10266A, Addendum A. In addition, the development processes and procedures similar to safety-related software is specified for PAS software.

Diversity Requirements

The PAS will be implemented with a commercial grade I&C platform that is not the TXS platform.

Data Communications

The functional units in the PAS interface to the PICS via networked connections.

The PAS ~~in the NI~~ may implement networked data connections between the CUs in each division to share signals as needed (e.g., to implement signal selection algorithms).

The PAS will have adequate bandwidth to reliably operate the process systems in the reactor plant needed for plant operation and to keep the plant reliably online.

Power Supply

The PAS is powered by the following power supplies:

- Safeguard Buildings - 12UPS.
- Turbine Building - non-Class 1E uninterruptible power supply (NUPS).
- Other buildings - UPS and diesel backed source.

The 12UPS provides backup power with 12-hour batteries and the SBODGs in the event of a LOOP.

The NUPS provides backup power with 2-hour batteries and the SBODGs in the event of a LOOP.

The PAS power supply contains redundant power supplies for both the cabinet chassis and the field devices. If one supply fails, the redundant supply automatically supplies the load without interruption to the PAS system and components. The intent is to minimize the possibility of a single failure in the non-safety-related system that will cause a transient or challenge a safety-related system.

Each supply is provided its own power supply feed from a separate source of power. The primary source of power to the PAS is provided by a critical battery-backed source. The secondary power source comes from a separate battery-backed source fed from a different power bus. In case of a total loss of power to the plant, the battery source permits continued operation of the plant controls for a period that allows safe shutdown of the process. The intent is to minimize the possibility of a single failure in the non-safety related system that causes a transient or challenge a safety-related system.

Replacement of supplies are permitted on-line without affecting operation.

Control voltage and field device voltage is 24 Vdc unless specified otherwise.

Battery-backed systems that provide power to the PAS are being monitored by the PAS for internal cabinet temperature/humidity and input/output voltages, with appropriate alarms for off normal conditions. The intent is an automatic surveillance function to identify degradation and, therefore, early repair of non-safety-related systems that may challenge safety-related systems.

The electrical power systems are described in detail in Chapter 8.

7.1.1.4.7 Diverse Actuation System (DAS)

The DAS is the non-safety-related I&C system that is provided to mitigate an AOO or PA concurrent with a CCF of the PS.

Classification

The DAS is classified as non-safety related, supplemented grade (NS-AQ).

Functions

Table 7.1-3 shows the functions of the DAS.

7.7.2.2.6 Feedwater Temperature Control

Main feedwater to each steam generator is temperature controlled to ensure sufficient heat removal from the primary coolant system and to prevent thermal stress on the steam generator itself. This temperature control is performed using several stages of feedwater heating by low-pressure heaters in the condensate system and high-pressure heaters in the Main Feedwater System.

Condensate pumps are utilized to move condensate from the low-, intermediate-, and high-pressure condensers to the low-pressure (LP) feedwater heaters (FWH) and then in to the deaerator/feedwater storage tank. There are two stages of LP FWH in the condensate system. The first stage consists of three parallel strings, each having two LP FWH in series. Each string contains two FWH bypass valves that operate in tandem to bypass the heaters. The warmed feedwater is passed through the first stage of heaters, combined via a common header, and then passed through the second stage of LP FWH. The second stage consists of two parallel strings, each having two LP FWH in series.

The MFW system contains the high-pressure (HP) feedwater heaters (FWH). There is one stage of HP FW heating. This consists of two parallel strings, each having two HP FWH in series. Each string contains two FWH bypass valves that operate in tandem to bypass the heaters.

The LP and HP FWH bypass valves are three-way valves that are provided such that each string can be isolated and bypassed. Relief valves are provided to protect the heat exchanger tube sides and associated piping from over pressurization due to thermal expansion of trapped fluid.

Each FWH is equipped with high- and low-level indicators to throttle open the appropriate drain valve when the condensate level in the FWH reaches either of the preset levels. Each FWH is also equipped with a high-high level indicator to send an alarm to the control room to indicate abnormal operation of the Feedwater Heater Drains System.

If the level in LP FWH A3 or LP FWH A4 of either train rises for any reason, the emergency drain control valve to the HP condenser of the respective LP FWH opens. If the level in one of the LP FWH A3 is too low, the associated LP FWH drain pump is tripped.

If the water level in the run-off loop of one of the LP FWH Al or A2 rises and reaches the specified setpoint, the corresponding FWH train will be automatically isolated. If the water level in LP FWH A3 or A4 rises above the control range of the emergency drain valve, the FWH train will be bypassed automatically and the flow is diverted to the second FWH train. If the water level in LP FWH A3 or A4 rises over the maximum setpoint, the main condensate pumps will be tripped.

If the water level in HP FWH A6 or HP FWH A7 of either train rises above the normal control range, the emergency drain control valve to the HP condenser of the respective FWH throttles open.

If the water level in HP FWH A6 or A7 rises above the emergency control range, the respective FWH train will be bypassed and the flow is diverted to the second FWH train. If the water level in any of the HP FWHs rises above the maximum level, the feedwater pumps are tripped.

7.7.2.3 Process Limitation I&C Functions

7.7.2.3.1 Loss of One Reactor Coolant Pump Limitation

This limitation function is designed to avoid the low reactor coolant system flow rate (i.e., one loop) reactor trip function described in Section 7.2.

This function initiates a PT and a turbine load reduction when two RCS loop flow values of the same loop drop below the setpoint value and the P3 permissive is validated.

7.7.2.3.2 Axial Offset Limitation

The objective of this limitation is to survey the azimuthal power imbalance and make sure that the axial power distribution is within the parameters assumed in the safety analysis to limit the consequences at high power levels of accidents or AOOs for which a top-peaked core power distribution is penalizing. The limited parameter is the AO value calculated from the self powered neutron detectors. The AO operating range is bounded by positive and negative thresholds. This function generates alarms and the blocking of the generator power increase.

This limitation function is inhibited below a low level of power.

The calculated AO is compared with thresholds derived from reactor power. When the threshold is met an action occurs to block the increase of generator power.

7.7.2.3.3 Reactor Power Limitation with Respect to Feedwater Flow Rate

This limitation function limits the reactor power with respect to the feedwater flowrate. The limitation function is designed to correct plant conditions before a protective action due to low SG level occurs. The loss of one or more main feedwater (MFW) pumps leads to a large imbalance between power generation in the reactor and heat transfer to the main heat sink. Process control I&C will detect the failure of one pump and start a standby pump, if available, within a few seconds, thus allowing normal operation to continue.

This limitation function can handle the following three events:

Functions assigned to RCSL ~~and PAS~~ are redundant in more than one division. The failure of a function in one division is backed up by a redundant function in another division. The redundant functions and their associated equipment, including support systems are independent of each other. Independence is achieved by the following:

- Redundant functions are allocated to physically separated divisions.
- ~~Electrical isolation between divisions.~~
- Erroneous signals or messages from one faulty division do not impair the functionality of the remaining divisions.

The RCSL is powered from the 12-hour UPS. During normal operation, the 12-hour UPS is powered from offsite power via the NPSS. In the event a LOOP occurs, the 12-hour batteries and the SBO diesel generators provide power to the severe accident portions of the RCSL.

Control functions assigned to each of the four independent PAS systems are segmented by CU pairs such that a control system failure in one CU pair of one PAS system will not propagate failure to any other CU pair or independent PAS system as whole. This segmentation reduces the probability of SWCCF such that SWCCF is not considered when analyzing PAS failures on the FSAR Chapter 15 Safety Analysis. No failure of PAS will affect all four divisions of PAS or initiate transients outside of the bounds of the Chapter 15 analysis.

Independence of each PAS division is achieved by the following:

- Segmented functions are uniquely allocated to each CU.
- Erroneous signals or messages from one faulty division do not impair the functionality of the remaining divisions or processor pairs.

~~The primary source of power to the RCSL and~~ PAS is powered~~provided~~ by a battery backed source. The secondary power source is from a separate battery backed source fed from a different power bus. Upon loss of the primary source of power to PAS ~~or RCSL~~, the secondary power source automatically and without interruption, maintains power. In case of a total loss of power to the plant, the battery source permits continued operation of the plant controls for a two hour period.

Segregation of functions is provided by allocating functions related to core control in the RCSL and functions related to RCS parameters in the PAS. Failures of components in one non-safety-related system do not a~~e~~ffect the functioning of the other non-safety-related system.

Control system failures are considered as event initiators in the safety analysis described in Chapter 15.