



December 16, 2009  
NRC:09:130

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

**Response to U.S. EPR Design Certification Application RAI No. 227, Supplement 5**

- Ref. 1: E-mail, Getachew Tesfaye (NRC) to Ronda Pederson, et al (AREVA NP Inc.), "U.S. EPR Design Certification Application RAI No. 227 (2564, 2598), FSAR Ch. 19," June 5, 2009.
- Ref. 2: E-mail, Russell D Wells (AREVA NP Inc.) to Getachew Tesfaye (NRC), et al., "Response to U.S. EPR Design Certification Application RAI No. 227, FSAR Ch 19," July 6, 2009.
- Ref. 3: E-mail, Ronda M. Pederson (AREVA NP Inc.) to Getachew Tesfaye (NRC), et al., "Response to U.S. EPR Design Certification Application RAI No. 227, FSAR Ch 19, Supplement 1," July 16, 2009.
- Ref. 4: E-mail, Ronda M. Pederson (AREVA NP Inc.) to Getachew Tesfaye (NRC), et al., "Response to U.S. EPR Design Certification Application RAI No. 227, FSAR Ch 19, Supplement 2," July 24, 2009.
- Ref. 5: E-mail, Russell D Wells (AREVA NP Inc.) to Getachew Tesfaye (NRC), et al., "Response to U.S. EPR Design Certification Application RAI No. 227, FSAR Ch 19, Supplement 3," August 27, 2009.
- Ref. 6: E-mail, Ronda M. Pederson (AREVA NP Inc.) to Getachew Tesfaye (NRC), et al., "Response to U.S. EPR Design Certification Application RAI No. 227, FSAR Ch 19, Supplement 4," September 17, 2009.

In Reference 1, the NRC provided a request for additional information (RAI) regarding the U.S. EPR design certification application (i.e., RAI No. 227). In Reference 2, AREVA NP Inc. (AREVA NP) provided responses to 12 of the 20 questions of RAI No. 262. In Reference 3, AREVA NP submitted Supplement 1 to provide a response to one of the remaining questions. In Reference 4, AREVA NP submitted Supplement 2 to revise the Supplement 1 related FSAR markup. In Reference 5, AREVA NP submitted Supplement 3 to provide a response to one of the remaining questions. In Reference 6, AREVA NP submitted Supplement 4 to provide a response to 3 of the remaining 6 questions. Technically correct and accurate responses to the remaining 3 questions are enclosed with this letter.

Appended to the response are affected pages of the U.S. EPR Final Safety Analysis Report in redline-strikeout format which support the responses to RAI 227 Questions 19-284 and 19-287.

DOTT  
NRC

**AREVA NP INC.**  
An AREVA and Siemens company

3315 Old Forest Road, P.O. Box 10935, Lynchburg, VA 24506-0935  
Tel: (434) 832-3000 Fax: (434) 832-3840

FORM 22700A-1 (4/1/2009)

The following table indicates the respective page(s) in the enclosure that contains AREVA NP's response to the subject questions.

Question #	Start Page	End Page
RAI 227 — 19-284	2	16
RAI 227 — 19-287	17	22
RAI 227 — 19-292	23	26

This concludes the formal AREVA NP response to RAI 227, and there are no questions from this RAI for which AREVA NP has not provided responses.

AREVA NP considers some of the material contained in the enclosure to be proprietary. As required by 10 CFR 2.390(b), an affidavit is enclosed to support the withholding of the information from public disclosure. Proprietary and non-proprietary versions of the enclosure to this letter are provided.

If you have any questions related to this submittal, please contact me. I may be reached by telephone at 434-832-2369 or by e-mail at [sandra.sloan@areva.com](mailto:sandra.sloan@areva.com).

Sincerely,



Sandra M. Sloan, Manager  
New Plants Regulatory Affairs  
AREVA NP Inc.

Enclosures

cc: G. Tesfaye  
Docket 52-020

AFFIDAVIT

COMMONWEALTH OF VIRGINIA            )  
  ) ss.  
COUNTY OF CAMPBELL                 )

1. My name is Sandra Sloan. I am Manager, Regulatory Affairs for New Plants, for AREVA NP Inc. and as such I am authorized to execute this Affidavit.

2. I am familiar with the criteria applied by AREVA NP to determine whether certain AREVA NP information is proprietary. I am familiar with the policies established by AREVA NP to ensure the proper application of these criteria.

3. I am familiar with the AREVA NP information contained in letter NRC:09:130, "Response to U.S. EPR Design Certification Application RAI No. 227, Supplement 5," and referred to herein as "Document." Information contained in this Document has been classified by AREVA NP as proprietary in accordance with the policies established by AREVA NP for the control and protection of proprietary and confidential information.

4. This Document contains information of a proprietary and confidential nature and is of the type customarily held in confidence by AREVA NP and not made available to the public. Based on my experience, I am aware that other companies regard information of the kind contained in this Document as proprietary and confidential.

5. This Document has been made available to the U.S. Nuclear Regulatory Commission in confidence with the request that the information contained in this Document be withheld from public disclosure. The request for withholding of proprietary information is made in accordance with 10 CFR 2.390. The information for which withholding from disclosure is

requested qualifies under 10 CFR 2.390(a)(4) "Trade secrets and commercial or financial information".

6. The following criteria are customarily applied by AREVA NP to determine whether information should be classified as proprietary:

- (a) The information reveals details of AREVA NP's research and development plans and programs or their results.
- (b) Use of the information by a competitor would permit the competitor to significantly reduce its expenditures, in time or resources, to design, produce, or market a similar product or service.
- (c) The information includes test data or analytical techniques concerning a process, methodology, or component, the application of which results in a competitive advantage for AREVA NP.
- (d) The information reveals certain distinguishing aspects of a process, methodology, or component, the exclusive use of which provides a competitive advantage for AREVA NP in product optimization or marketability.
- (e) The information is vital to a competitive advantage held by AREVA NP, would be helpful to competitors to AREVA NP, and would likely cause substantial harm to the competitive position of AREVA NP.

The information in the Document is considered proprietary for the reasons set forth in paragraphs 6(b) and 6(c) above.

7. In accordance with AREVA NP's policies governing the protection and control of information, proprietary information contained in this Document has been made available, on a limited basis, to others outside AREVA NP only as required and under suitable agreement providing for nondisclosure and limited use of the information.



**Response to**

**Request for Additional Information No. 227, Supplement 5**

**6/05/2009**

**U. S. EPR Standard Design Certification**

**AREVA NP Inc.**

**Docket No. 52-020**

**SRP Section: 19 - Probabilistic Risk Assessment and Severe Accident Evaluation**

**Application Section: 19**

**QUESTIONS for PRA Licensing, Operations Support and Maintenance Branch 1  
(AP1000/EPR Projects) (SPLA)**

**Question 19-284:**

(Follow-up to Question 19-68) The staff needs additional information on the software common-cause failures (CCF) modeled in the U.S. EPR probabilistic risk assessment (PRA) to conclude that the low postulated failure rates do not result in an over-optimistic estimation of risk. Specifically:

- a. The assumed software CCF probabilities can be found in Final Safety Analysis Report (FSAR) Table 19.1-13, but not in the text of Section 19.1.4.1.1.3 where digital instrumentation and control (I&C) modeling is discussed. Revise the FSAR to state the software CCF probabilities assumed.
- b. Page 19.1-34 of the FSAR states that the TELEPERM XS (TXS) "operating history...is used to generate a bounding value" for the operating system CCF probability. Interim Staff Guidance (ISG) DI&C-ISG-03 cautions that "extrapolation of statistical data of the same system used in a different operating environment or profile is not necessarily meaningful." Discuss how this bounding value was developed, including a justification of the applicability of operating history to a new environment in which a different set of input parameters could reveal a fault not exposed in the previous operating history. Revise the FSAR to include a summary of this information, and confirm that all important assumptions implicit in the operating system CCF value are included in FSAR Table 19.1-109.
- c. Page 19.1-34 states that application software CCF probabilities are "based on comparison of the software development...process and the TXS platform design characteristics with applicable international standards." Revise the FSAR to describe the specific process and design characteristics that contribute to the low application software CCF probability. Discuss how the software development process supports the assumption that the application software in diversity groups A and B can be considered independent in the PRA, given the use of "qualified software functional blocks from a controlled library." Confirm that all important assumptions implicit in the application software CCF value are included in FSAR Table 19.1-109.
- d. Confirm whether the error factor of five used for digital I&C equipment (stated in FSAR Section 19.1.4.1.2.7) was also applied to the operating system and application software CCFs. Justify the uncertainty parameters applied to software CCFs given the limited state of knowledge about these failures. Revise the FSAR to include a summary of this information.
- e. The sensitivity studies performed in response to Question 19-68 provide useful information on the effect of modeling uncertainty on the at-power core damage frequency (CDF). However, the effect of these sensitivity cases on both CDF and large release frequency (LRF) resulting from all modes of operation is unclear. Provide CDF and LRF results from the fourth sensitivity case for both at-power and shutdown modes.
- f. In the sensitivity studies performed in response to Question 19-68, the operating system and application software CCF probabilities are increased by one order of magnitude (to 1E-6 and 1E-4, respectively). So that the staff can understand the importance of low software CCF probabilities to the overall risk profile, provide the CDF and LRF results from a sensitivity study in which these probabilities are increased to demonstrably conservative values (e.g., 1E-4 and 1E-3).

**Response to Question 19-284:****Response to Question 19-284, Part a:**

U.S. EPR FSAR Tier 2, Section 19.1.4.1.1.3 will be revised to include a statement of the software common-cause failure (CCF) probabilities assumed.

**Response to Question 19-284, Part b:****Applicability of TXS Operating System (OS) History**

TXS is AREVA NP's instrumentation and controls (I&C) system platform for safety-related I&C. The first TXS systems were put into operation more than ten years ago and have been working reliably. TXS I&C systems have been installed in 39 units at 24 plant sites located in 11 countries and utilizing 10 different reactor designs. TXS OS operating experience is applicable for use in the U.S. EPR environment.

The operating history of the TXS OS is applicable to a new environment (i.e., application) that has different input parameters. Use of a different set of input parameters does not affect applicability of the OS operating history because:

- Unlike the application software, the TXS OS is not configured to be used in a specific application. It is a standard OS used in TXS applications.
- There is no interface between the OS and the power plant (i.e., input parameters). This interface is implemented in the application software.
- The TXS platform is designed to prevent interference from input parameters or application software on the operation of the OS, as described in this response.

The TXS platform is designed with specific features that result in reliable and predictable performance of the OS and behavior that is free of interference from either the application program or from external plant transients. These features are discussed in Topical Report EMF-2110(NP)(A), referenced in U.S. EPR FSAR Tier 2, Section 7.1.1.2.1, and summarized in Part c of this response. Key features of OS reliability include:

- Strictly cyclic operation.
- Constant bus loading.
- Static memory allocation.
- No process-dependent interrupts.

These features provide reasonable assurance that event- or environment-related failure triggers, caused by special loading (operation outside of anticipated limits), unanticipated input signal trajectories (change of input signals over time), or application program design errors (e.g., incorrect setpoints, specification errors), will not affect the OS, and consequently propagate a failure to redundant or diverse functions.

The TXS design forces a dissociation of the OS, both from the application software and from external plant transients, which protects against event- or environment-related failure triggers of the OS software. These design features are important for defense against CCF as reinforced



by IEC-62340 (Reference 1), the industry good practice document for defense against CCF in safety-related digital I&C design.

### **Evaluation of TXS OS Failure Probability**

As discussed in U.S. EPR FSAR Tier 2, Section 19.1.4.1.1.3, TXS design features, such as deterministic program execution, constant bus loading, and cyclic operation, preclude demand-related stresses from affecting the OS. In addition, they disconnect the performance of the OS from signal trajectories and potentially untested data sets. This is significant for the quantification of OS failure probability because it:

- Removes application-specific variability from OS reliability.
- Removes demand-related stress from the OS reliability.
- Allows the OS portion of the failure probability to be calculated based on the previous operating history. (Application software failure probability is addressed in Part c of this response.)

The bounding value for CCF probability of the OS was developed using the history described above. The computer processor modules had over 62 million operating hours of accumulated experience through 2006. During this time, there were [ ] random failures of the computer processor modules, and no OS failures. The accumulated processor operating experience is 92 million hours through 2008, with no additional failures. However, the data through 2006 was used and an OS failure rate of less than one per 62 million hours is indicated, or less than [ ] per hour. Using a chi-squared distribution with 95 percent confidence level provides an upper bound OS failure rate of approximately [ ] per hour. This represents the upper bound OS failure rate for a single computer. Although there is no identified mechanism for simultaneous OS failure in multiple independent and asynchronous computers, the PRA makes the conservative assumption that the 95 percent chi-squared failure rate of a single OS represents a CCF of the 48 computer processor modules in the PS (i.e., beta-factor = 1.0).

The unavailability (or failure probability) for the OS CCF is determined from the failure rate and the downtime (or time of vulnerability) that results if there is a postulated CCF of the OS in the field (i.e., lockup of multiple computer processors in redundant channels). The failure will be self-evident and prompt immediate action to reboot the computers or initiate plant shutdown. A Technical Specification limiting conditions for operation (LCO) is triggered with a short completion time (i.e., one hour). Allowing one hour for the downtime yields an unavailability of [ ], rounded to 1E-7 for the OS CCF probability.

U.S. EPR FSAR Tier 2, Section 19.1.4.1.1.3 will be revised to include a discussion of how the OS failure probability was developed and why it is applicable. U.S. EPR FSAR Tier 2, Table 19.1-109 will be revised to add an assumption to acknowledge the importance of the TXS CCF defenses.

### **Response to Question 19-284, Part c:**

Safety-related I&C applications developed on the TXS platform have low CCF potential. Process and design characteristics of TXS that contribute to low application software CCF probability include:

1. High quality software development lifecycle process.
2. Robust platform design characteristics, including:
  - OS features that minimize failure triggers.
  - OS features that prevent application software failures from propagating to other functions.
3. Functional diversity.

These defenses against CCF conform to generally-accepted industry good practice, as discussed in Reference 1. The multi-pronged defense is used because software failure requires a latent defect in the application software, as well as something in the data trajectory to trigger the failure. Prevention of CCF also involves reducing failure consequence. The software development lifecycle process that reduces software defects is significant to application software reliability. The features of the platform and OS software that reduce the triggers for application software failure, and the features that prevent propagation of application software failures to the broader system, are also significant. This section discusses the platform design and application software development process for TXS. See Topical Report EMF-2110(NP)(A) for additional information.

#### **Platform Design Features that Minimize Failure Triggers and Prevent Propagation of Application Software Failures**

The TXS platform has features that reduce the triggers for application software failure and features that prevent propagation of application software failures to the broader system. Some of these features are discussed in Part b of this response. For example, application software defects can be triggered by unanticipated signal trajectories or data sets. Deterministic program execution coupled with cyclic processing results in an unvarying path through the software that is the same whether there is a demand or not. The program execution cycles through the function blocks (see the function block discussion in this response) in a repeating pattern that is not altered by signal trajectories or data sets. Failure can also occur from software defects that are triggered by "special loading." Cyclic processing and invariable loading of processor and communication buses provide reasonable assurance that "data storm" events (network or processor overload due to demand challenges and competing application programs) are not possible. Another potential trigger of software defects is interference between the application program and the OS. Features, such as static memory allocation, eliminate the possibility of OS halt due to conflicts in dynamic memory allocation. Process-driven interrupts are also not allowed. These features and others provide separation of the OS from the application software. Failure consequences are reduced or contained by not allowing an application program failure to affect the OS and consequently propagate to redundant channels or diverse functions.

The TXS platform software has been designed for high reliability. The applied defense-in-depth design strategy:

- Avoids system errors by using a modular system with relatively simple and testable components.
- Avoids design errors by stipulating a clear design process with a phase structure including verification and validation (V&V) steps.
- Copes with system failures utilizing self-monitoring and fault handling routines.

The TXS system software comprises a set of type-tested modules, which are used exclusively in the implemented systems. The application functions are designed with the SPACE (specification and coding environment) tools as function diagrams by selecting and connecting the appropriate function block modules available from a function block library. For each processing module, the application software code is generated from this specification (function diagram modules) and then linked to the standard system software resulting in a runtime architecture.

The application functions are controlled by the runtime environment (RTE) and are separated from the OS software and services (OS is MICROS; communication software package is MicroNET) and hardware-specific software such as input/output drivers and communication protocol handlers. This independence is a key feature for configuration management and maintenance of the system platform, allowing integration of new hardware components (processor boards, I/O boards, etc.) without affecting the functionality of the application.

The generic interface between application functions and the system software is generated during project engineering by a SPACE code generation tool. It automatically creates the call and data interface to the function diagram modules and describes the I/O and communication activities that have to be performed by the processing module.

The deterministic behavior of integrated I&C systems important to safety is based on a set of features of the TXS system platform (platform hardware, system software, and platform tools) in combination with specific design principles. To provide the required deterministic behavior with respect to safety, the following four requirements have to be met:

- The software is processed on each CPU in a strictly cyclic manner independent of any input data trajectory. The time required for processing the specified software on each CPU is limited and designed to be below the cycle time.
- The communication between the processing units inside of a TXS based I&C system, as well as with outside systems, is performed in a strictly cyclic manner and interference-free based on communication with minimal coordination. Postulated failures of a sending CPU or a communication device cannot influence the cyclic operation of a receiving CPU. The communication with minimal coordination is an effective barrier against fault propagation.
- The processing of plant process data is performed so that no data-triggered interference is permitted to cause CPU overload or failure (e.g., software exception).
- The operation of the system software does not disturb the strictly cyclic processing of the application software and protects against system dead-lock situations in each CPU.

Strict separation between system software and application software reduces the probability that postulated latent errors may be triggered to cause system failure. The following design principles also improve the reliability of system operation:

- No real-time clock - To exclude any interference of the cyclic functional task processing with any calendar dates or clock-based events, no real-time clock is used in the system. Instead, the cycle time being specified for each CPU as a multiple of the 1ms hardware timer pulse is used as time basis for all time-dependent application functions. The cycle time specified is flexible between five and 1600 milliseconds (50 ms is typical), depending on process requirements. A 16 bit cycle counter is individually handled by each CPU and incremented every processing cycle.

- Static memory allocation - All memory resources of the application software are defined during code generation. Required data buffers are allocated statically in the generated code. Each data buffer has only one purpose. The code is allocated in ROM and executed directly from ROM. The data areas allocated statically are put by the compiler into separate data segments which are allocated in RAM. All memory resources of the system software (e.g., data buffers for communication) are allocated statically in system software RAM and in communication RAM and are configured during CPU startup. They are not modified or freed after startup. There is no dynamic allocation of memory resources. Therefore, dead-lock situations due to depletion of resources are prevented.
- No process-dependent interrupts - As a basic design principle of TXS, no process-dependent interrupt is applied or possible. This feature avoids adverse effects, which could be triggered by unfavorable input signal trajectories.
- Cyclic Operation - On startup of a CPU, an initialization routine is executed. After successfully passing comprehensive self tests, the CPU is switched to its normal status commencing cyclic operation. The engineered cycle time is controlled by the internal system clock, which provides the time basis using interrupts at one-millisecond intervals.
- Measures against software exceptions - Measures to avoid software exceptions during cyclic processing are implemented in the system software as well as the application software. The functions provided by the system-software (e.g., the transfer of messages, check of received messages, buffering of data, and transfer of I/O signals) are implemented so that the correct execution of these software functions cannot be disturbed by any combination of values of the process-dependent data being processed. Pre-checks and remedial actions are implemented in the software to protect CPUs against software exceptions from application software processing. The following situations are captured and handled by well-defined standard system actions:
  - Input data range violation - Input data range violations of the analog-digital converter are detected and indicated by the I/O driver controlling the input board. An input data range monitoring function can also be engineered for each data as a part of the application software.
  - Not-a-number (NAN) strings in data messages (i.e., invalid floating point data) - Data messages received from other CPUs are checked prior to processing of received data. Besides message header, age and cyclic redundancy check (CRC) data checks, a NAN check of floating point data is performed to prevent floating point exceptions caused by invalid application data (e.g., division by zero, exponent of negative values, square root of negative values, and result overflow or underflow of float point operations).

To provide safe processing of plant-specific data, algorithms are implemented in the TXS function block modules to prevent exceptional situations by pre-checking and substituting suitable values for computation, when needed. Additionally, a fault indication is sent to the service unit (SU) in case of an abnormal situation.

In TXS, there are two ways of detecting failures:

- Failure detection by self-monitoring mechanisms as an inherent feature of the system platform.
- Detection by configured/engineered monitoring functions.

The inherent mechanisms use monitoring equipment to identify deviations from the expected system behavior. This is implemented independently of the specific application and includes monitoring of:

- Power supply and environmental temperature.
- Waiting time for allocation of the backplane bus.
- Access time and time-out on access to the backplane bus (bus arbiter).
- Cyclic operation of function processors (watchdog).
- Hardware functions of the processing units (self-test task).
- Cyclic communication (message age monitoring, CRC-check).
- Consistency of data processing in master and checker CPUs (when used).

In configured failure monitoring, deviations in redundant application-specific information are used to detect failures both in the TXS equipment system and in the peripheral sensing equipment. These configured monitoring functions are supported by the platform capability of maintaining a status signal with each data signal that is processed in the application software. Detected faulty (or missing) input signal data of a function processor are marked as faulty. In processing signal data, the function blocks include the processing of the signal status in a pre-defined manner. Specific functions are available to exclude incorrect information from further processing and propagation. Examples are:

- Function blocks for on-line signal validation and voting logics.
- Function blocks defining a fail-safe action in case of faulty input data.
- Suppression of faulty data to output boards and replacement with a fail-safe action.

The application of SPACE engineering tools is mandatory to specify the safety functions together with the detailed architecture of the target system. The SPACE engineering tools are also used to generate the application software, which is loaded to the processing units of the safety I&C target system (after compiling, linking, and locating the code). The code generator tools have been designed and qualified for the creation of safety application software (ANSI C source code). They include a variety of checks of the specification data and follow strict design rules for the generated code meeting IEC-60880 (Reference 2) stipulations. The project-specific software is generated through these tools to provide reasonable assurance that the design rules and interfaces defined for TXS application software functions are met. This is also a precondition to support efficient software configuration management and V&V.

### **High Quality Software Development Lifecycle Process**

The application software development lifecycle process for TXS is designed to reduce the potential for software defects. TXS is a mature safety-related I&C platform with a structured and well-controlled application software development process. The TXS platform design includes software development tools to automate application software development and reduce human error. The application programming is also restricted to the use of software functional blocks from a controlled library, which is qualified and tested. A rigorous V&V process demonstrates that application program functional requirements are complete and correct, and that they are

correctly implemented. There are also configuration control requirements for modification of the software after its initial installation.

Topical Report ANP-10272, "Software Program Manual for TELEPERM XS Safety Systems," describes the programs and measures incorporated to:

- Provide reasonable assurance that the TXS application software attains a level of quality commensurate with its importance to safety-related functions.
- Provide reasonable assurance that the application software performs the required safety-related functions correctly.
- Conform to established technical and documentation requirements, conventions, rules, and industry standards.

The Software Program Manual describes the requirements and objectives for the following plans that are recommended in BTP 7-14:

- Software Management Plan, which describes the overall management process used for the development of project-specific TXS application software.
- Software Development Plan, which describes the lifecycle activities for TXS application software development.
- Software Quality Assurance Plan, which describes the necessary processes that provide reasonable assurance that the software attains a level of quality commensurate with its safety-related function.
- Software Integration Plan, which describes the software integration process and the hardware/software integration process for TXS projects.
- Software Installation Plan, which describes the installation process for TXS projects.
- Software Operations and Maintenance Plan, which describes post-customer delivery TXS software practices.
- Software Training Plan, which describes a process that can be used to provide reasonable assurance that training needs of appropriate plant staff, including operators and I&C engineers and technicians, are met.
- Software Safety Plan, which identifies the process to reasonably eliminate hazards that could jeopardize the health and safety of the public from safety-critical software.
- Software Verification and Validation Plan, which describes the method that verifies correctness of the TXS application software.
- Software Configuration Management Plan, which describes the method that maintains the project-specific TXS software in a controlled configuration.
- Software Test Plan, which describes the purpose and scope of the TXS application software testing activities.

The requirements for safety-related I&C software defined in Reference 2 form the basis for the TXS features described in this section. Reference 2 requires a structured development process with documentation of the design and development steps, as well as V&V of the development

results in accordance with the phase model. The development of the safety-related software components of TXS conforms to these standards.

TXS safety-related I&C systems reuse the same tested and qualified software components (function blocks) repeatedly. The engineered functions are based on preprogrammed modules in the standardized function block library, which are interconnected by an automatic code generator. The engineering data specified on function and hardware diagrams and stored in the project database are used as input. Manual programming is not necessary or allowed. This approach provides reasonable assurance that simple code structures are produced that fulfill the highest test requirements and that the implemented function is documented in graphical form.

The reusable software components (i.e., the function blocks) and system software components have been qualified generically and plant-independently consistent with German KTA 3503 (Reference 4). Similar to the hardware qualification, software qualification also consists of analytical investigations and practical tests.

The theoretical tests performed by the German Institute of Safety Technology (GRS/ISTec) and German Technical Inspection Agency (TÜV Nord) have proven that:

- The development documentation is consistent from the requirement specification through to the design and implementation documentation.
- The required tests have been performed and appropriately documented.
- The software complies with the required design principles.

The generated code is subjected to a tool-based analysis and checked for compliance with specifications.

### **Functional Diversity and Function Blocks**

Functional diversity defends against unforeseen failures caused by functional specification faults (functional and other diversities employed by the U.S. EPR I&C design are described in U.S. EPR FSAR Tier 2, Sections 7.1.1.6.2, 7.7.2.11, and 7.8). Functional diversity (provided by the A and B diversity groups) is most effective when coupled with a platform design that includes the other defenses, which prevent failures from propagating to redundant or diverse functions, channels, and subsystems.

Software function blocks are important for the reliability of the application software and do not compromise the independence of the A/B diversity groups used in the PS.

The A and B subsystems of the PS provide functional diversity. The functions assigned to the two diversity groups have different functional specifications, different sensed parameters, and different signal trajectories. Reference 1 endorses functional diversity as an effective defense against application-specific software faults such as specification errors. By introducing different signal trajectories, function diversity also protects against common failure triggers.

The medium for communication of application-specific functional specifications is a functional diagram (implemented and standardized via the SPACE engineering tool). The application-specific software is built with these functional diagrams, which use the pre-qualified graphically-

represented functional blocks. The application software designer (I&C engineer) has control of the program code only via these function block diagrams, so there is no manual development of software programming "statements."

The function diagrams are composed of function blocks that represent simple functions, which are verified and tested. The function block library is a limited collection basic I&C functions such as "limit signal generator," "adder," or "integrator." Numeric and logical operations on signals are only performed within the function block modules. The function block diagram is readily understood by both the process engineers and the I&C engineers responsible for the application software.

The application software designer has no access to the programming within the functional blocks. These function blocks are generated with a subset of the C programming language, and are present as qualified binary coded components. The programming logic within the functional block is thoroughly tested during the qualification process. Because the same function blocks are used and tested repeatedly in many applications, there is high confidence that they are error free.

In execution, the runtime environment operates cyclically, executing the entire set of function blocks several times per second (20 times per second is a typical cycle). Each incarnation of a function block module has a static connection with a data structure that contains dedicated locations for the input data and output data as well as the internal buffers and parameters. The functional diagram programming is implemented as a linear sequence of function block modules that are linked by suitable data structures.

At the functional diagram level, which is where the application-specific programming occurs, every path is executed on each program cycle. The reaction to demands from the plant process changes only the data in the application software, via the dedicated function block inputs. One consequence of cyclical system processing is that the task processing time and the communication load are set during configuring and are not affected by demands for system response.

Specification errors, if they are introduced, occur in the user-defined input, which is at the functional diagram level. At this level, the A/B functional diversity addresses the potential vulnerability introduced by the application engineer via weaknesses in specifications or analytical knowledge. It does not address postulated vulnerability introduced by the function blocks programming, hardware, or other system vulnerabilities. In terms of the CCF probabilities used in the PRA, the application software CCF probability addresses the first vulnerability (e.g., function specification errors) and the OS CCF probability addresses the second vulnerability (e.g., OS or function block errors).

U.S. EPR FSAR Tier 2, Chapter 19 will be revised to clarify the PRA modeling assumptions with respect to the A/B diversity.

A sensitivity case was performed modeling a dependency between the application software in diversity group A and B. This dependency was modeled with a beta-factor of 0.1. The results are shown in Table 19-284-1.



## Evaluation of Application Software Failure Probability

As discussed in U.S. EPR FSAR Tier 2, Section 19.1.4.1.1.3, the application software CCF probability is assigned based on subjective engineering judgment. These judgments are based on the lifecycle processes for application software development and platform design characteristics being comparable to:

- Reference 1 standards of good practice for defense against CCF.
- Reference 2 standards of good practice for software.
- IEC-61508 (Reference 3) standards of good practice for safety integrity level (SIL) four (SIL-4).

Reference 3 defines SIL as a relative level of risk reduction, which is assigned based on requirements in two broad categories: hardware safety integrity and systemic safety integrity (i.e., software). The TXS platform and reactor protection system (RPS)/engineered safety feature actuation system (ESFAS) applications on the TXS platform are qualified to a rigorous SIL, which is SIL-4. Reference 3 also provides risk targets, which for a SIL-4 system correspond to a failure probability between  $1E-4$  and  $1E-5$  per demand. The risk target values were used as a general guide to assign a reasonable application software failure probability based on engineering judgment. Because the target values apply to the combined hardware and the software system, engineering judgment was used to allocate half of the target range (between  $5E-5$  and  $5E-6$ ) to the software. Within this range, a value of  $1E-5$  was chosen for the application software failure probability in each of the diversity groups.

U.S. EPR FSAR Tier 2, Chapter 19, including Table 19.1-109, will be revised to enhance the discussion of the assumed application software CCF probabilities and their relationship to compliance with these standards.

Even though the application software in redundant channels of the same diversity group is the same, simultaneous failure is not a certainty. OS defenses, such as asynchronous operation, are designed to reduce the likelihood of a common failure trigger in redundant channels. To be conservative, the PRA makes the assumption of complete dependence between redundant channels of identical software, and the assigned application software failure probability is applied in the PRA as a CCF of the applicable diversity group.

As indicated in the Response to RAI 7, Question 19-67, a recovery probability of 0.5 was applied to the application software CCF probability in order to conservatively compensate for the effect of the diversity and defense-in-depth (D3) functions, which have not been incorporated into the PRA. The D3 functions are backup automatic and manual actuations that are intended to mitigate software CCF.

### Response to Question 19-284, Part d:

An error factor of five (lognormal distribution) was not used for application software and operating system CCF.

CCF probabilities for the OS and application software used a constrained non-informative (CNI) distribution. Because the software CCF probabilities are based on limited information, the CNI distribution models uncertainties in the estimated values. The CNI distribution applies because

there is a large uncertainty in the value of the parameter, and the shape of the distribution is unknown. As explained in U.S. EPR FSAR Tier 2, Sections 19.1.5.2 and 19.1.5.3, the CNI distribution was also used for fire and flood initiating event frequencies.

U.S. EPR FSAR Tier 2, Section 19.1.4.1.2.7 will be revised to clarify that a CNI distribution was used for operating system and application software CCFs.

Although the uncertainty in software reliability estimates is high for all new plant applications, the maturity of the TXS platform offsets this uncertainty. The ten-plus years of operating experience in safety systems of 39 different nuclear power plants (see Part b of this response) is directly applicable and proves the effectiveness of the OS failure defenses and of the lifecycle processes for application software development.

**Response to Question 19-284, Part e:**

Sensitivity case 4 from the Response to RAI 7, Question 19-68 has been re-run to provide additional cases. New cases are LRF at power, CDF at shutdown, and LRF at shutdown.

As described in the Response to RAI 7, Question 19-68, sensitivity case 4 involves:

1. The software CCF probabilities are increased by one order of magnitude (10X).
2. The 0.5 software CCF recovery probability (see the Response to RAI 7, Question 19-67) is eliminated. (Net increase is 20X for application software, 10X for operating system.)
3. Beta-factors for CCF of digital components are increased by a factor of two (2X).
4. Human error probabilities (HEPs) associated with cut sets involving CCF of DI&C (including software) are increased by one order of magnitude (10X).

The results of the sensitivity cases are provided in Table 19-284-2.

**Response to Question 19-284, Part f:**

Sensitivity case 1 from the Response to RAI 7, Question 19-68 has been re-run with an increase in the OS and application software CCF probabilities. In this sensitivity case:

1. OS CCF probability is increased from 1E-7 to 1E-4 (1000X).
2. Application software CCF probability is increased from 1E-5 to 1E-3 (100x).
3. The 0.5 software CCF recovery probability (see the Response to RAI 7, Question 19-67) is eliminated. (Net increase is 200X for application software, 1000X for operating system.)

The results of the sensitivity cases are provided in Table 19-284-3.

Table 19-284-3 shows sensitivity to the probability assumed for software CCF. This result is expected, given the relatively high risk achievement worth (RAW) importance measures reported in U.S. EPR FSAR Tier 2, Tables 19.1-13 and 19.1-35, for OS and application software CCF. These results do not include credit for any diverse automatic or manual actuations that may be required for D3, other than diverse reactor trip (RT) (for the anticipated transient without scram (ATWS) rule). The diverse actuation system (DAS) will be designed to meet the BTP 7-19 diversity requirements as described in U.S. EPR FSAR Tier 2, Chapter 7.

**References for Question 19-284:**

1. IEC-62340, Nuclear Power Plants – Instrumentation and Control Systems Important to Safety – Requirements to Cope with Common Cause failure (CCF), Edition 1.0, International Electrotechnical Commission, 12-7-2007.
2. IEC-60880, Nuclear Power Plants – Instrumentation and Control Systems Important to Safety – Software Aspects for Computer-Based Systems Performing Category A Functions, Edition 2.0, International Electrotechnical Commission, 5-9-2006.
3. IEC-61508, “Functional Safety of Electrical / Electronic / Programmable Electronic Safety-Related Systems,” International Electrotechnical Commission.
4. KTA 3503 , “Type Testing of Electrical Modules for the Reactor Protection System”. Nuclear Safety Standards Commission (KTA), Germany.

**FSAR Impact:**

U.S. EPR FSAR Tier 2, Section 19.1.4.1.2.7, Section 19.1.4.1.1.3, and Table 19.1-109 will be revised as described in the response and indicated on the enclosed markup.

**Table 19-284-1—Results of Sensitivity Cases for Digital I&C: Dependency between Subsystem A and B Software CCF**

Mode	Sensitivity Case Description	CDF (1/year)	Delta CDF
At Power	0.1 beta factor between diversity group A and B software CCF	5.3E-07	1%
Shutdown	0.1 beta factor between diversity group A and B software CCF	5.8E-08	0%

**Table 19-284-2—Results of Sensitivity Cases for Digital I&C: Sensitivity Case 4 from Question 19-68**

Mode	Sensitivity Case Description	Original Model		Modified Model (Note 1)
		CDF (1/year)	LRF (1/year)	LRF (1/year)
At Power	Base Case	5.26E-07	2.60E-08	1.38E-08
At Power	Software 10X increase No software recovery Digital 2X beta increase HEP 10X increase	1.1E-06	1.3E-07	2.58E-08
Shutdown	Base Case – Shutdown	5.77E-08	5.70E-09	-
Shutdown	Software 10X increase No software recovery Digital 2X beta increase HEP 10X increase	6.2E-08	6.7E-09 (Note 2)	-

## Notes for Table 19-284-2:

1. This LRF is based on the sensitivity case from the Response to RAI 22, Question 19-160. An initial examination of the top At Power LRF cut sets reveals the LRF is impacted (>90 percent) by the initiator steam line break inside containment (SLBI). As presented in the Response to RAI 22, Question 19-160, the baseline At-Power LRF model assumes overly conservative consequences from SLBI. Sensitivity cases for this question also present results using the Response to RAI 22, Question 19-160 sensitivity case model. The contribution to At-Power CDF from SLBI is not significant.

2. This value is conservative because it does not credit the low head safety injection (LHSI) heat exchanger(s) in the cases where LHSI is available (safety injection system (SIS) failed due to I&C), but the severe accident heat removal system (SAHRS) is unavailable.

**Table 19-284-3—Results of Sensitivity Cases for Digital I&C: Larger Perturbation of Sensitivity Case 1 from Question 19-68**

Mode	Sensitivity Case Description	Original Model		Modified Model (Note 1)
		CDF (1/year)	LRF (1/year)	LRF (1/year)
At Power	Base Case	5.26E-07	2.60E-08	1.38E-08
At Power	OS CCF = 1E-4 App. Software = 1E-3 No software recovery	8.1E-06	1.2E-06	6.2E-08
Shutdown	Base Case – Shutdown	5.77E-08	5.70E-09	-
Shutdown	OS CCF = 1E-4 App. Software = 1E-3 No software recovery	1.3E-07	1.9E-08 (Note 2)	-

Notes for Table 19-284-3:

1. This LRF is based on the sensitivity case from the Response to RAI 22, Question 19-160. An initial examination of the top At Power LRF cut sets reveals the LRF is impacted (>90 percent) by the initiator SLBI. As presented in the Response to RAI 22, Question 19-160, the baseline At-Power LRF model assumes overly conservative consequences from SLBI. Sensitivity cases for this question also present results using the Response to RAI 22, Question 19-160 sensitivity case model. The contribution to At-Power CDF from SLBI is not significant.
2. This value is conservative because it does not credit the LHSI heat exchanger(s) in the cases where LHSI is available (SIS failed due to I&C), but the SAHRS is unavailable.

**Question 19-287:**

(Follow-up to Question 19-259) The response to Question 19-259 discusses the undeveloped basic events used for the process automation system (PAS) and safety automation system (SAS). It appears that, other than the sensors that may provide input to both the protection system (PS) and these systems, no dependency is assessed between the PS and PAS or SAS. The descriptions of all three systems, as well as that of severe accident (SA) I&C, in FSAR Section 7.1 state that they include "subracks, I/O modules, function processors, and communication modules, and optical link modules." The staff needs additional information to understand how these systems are modeled in the PRA.

- a. List the systems or functions (e.g., EDG actuation, partial cooldown) that the PRA assumes are actuated by each I&C system. For systems or functions actuated by the PS, state which diversity group is assumed to support the actuation.
- b. Describe all scenarios that include independent failures of both PS and another digital I&C system (e.g., PAS, SAS, SA I&C).
- c. Discuss whether CCFs of I&C components, which are modeled in detail for the PS, could be expected to affect PAS or SAS as well. If so, how is this dependence modeled in the PRA?

**Response to Question 19-287:****Response to Question 19-287, Part a:**

The functions assumed for each instrumentation and controls (I&C) system and for the A and B diversity groups of the PS are discussed in this response. This list is limited to the functions that are currently modeled in the probabilistic risk assessment (PRA).

As indicated in U.S. EPR FSAR Tier 2, Table 19.1-109, the PRA uses simplified models for some of the I&C functions because the detailed design of the associated I&C systems will occur later in the design process. For the PAS, SAS, and SA I&C, the PRA models will be developed in parallel with the detailed design.

**PS diversity group A functions modeled in the PRA:**

- Emergency feedwater (EFW) actuation.
- EFW level control (open/close wide-band).
- Emergency diesel generator (EDG) actuation.
- Reactor trip (RT) on high reactor coolant system (RCS) pressure.
- RT on low departure from nucleate boiling ratio (DNBR).

**PS diversity group B functions modeled in the PRA:**

- Safety injection system (SIS) actuation.
- Partial cooldown (PCD) actuation.
- Main steam relief train (MSRT) actuation (high pressure).

- MSRT isolation.
- Main feedwater (MFW) isolation.
- Main steam isolation valve (MSIV) actuation.
- EDG actuation.
- Containment isolation system (CIS) actuation.
- RT on high steam generator (SG) pressure.
- RT on low SG level.
- SG isolation on high level.

**PAS functions modeled in the PRA:**

- Reactor coolant pump (RCP) non-safety-related (NSR) automatic stop signals. For example, on high thrust bearing temperature, high thermal barrier temperature, and low thermal barrier flow.
- RCP standstill seal system (SSSS) actuation.
- MFW/startup and shutdown system (SSS) NSR control.
- Chemical and volume control system (CVCS) control (for RCP seal injection).
- CVCS letdown isolation on low (mid-) loop level.
- Residual heat removal (RHR) isolation on high sump level (pipe break).
- Operational chilled water (for normal heating ventilation and air conditioning (HVAC)).
- Closed loop cooling water system and service water system (for MFW cooling).
- Demineralized water system (for spent fuel pool makeup and MFW/SSS makeup).

**SAS functions modeled in the PRA:**

- Control of EFW level (narrow band).
- MSRT pressure control (i.e., control of PCD rate after actuation).
- RHR low suction pump trip.
- EDG control.
- Safety-related controls for component cooling water (CCWS), essential service water system (ESWS), and ultimate heat sink (UHS) fan.
- Control of signals to the extra borating system (EBS).

**SAI&C functions modeled in the PRA**

The SAI&C has no automatic actuation functions. The SAI&C system supports manual actions and monitoring functions for SA mitigation.

The PRA does not explicitly model the SAI&C system. The detailed designs for implementation of manual actuations and for SAI&C will occur later in the design process. The PRA for design

certification does not include explicit modeling of I&C to support operator actions. As explained in the Response to RAI 7, Question 19-71 and in U.S. EPR FSAR Tier 2, Table 19.1-109, Item 45, the PRA assumes that there is sufficient redundancy and diversity in the human machine interface (HMI) systems that control room indication is not a significant contributor to the HRA or the PRA. According to this assumption, there is sufficient redundancy and diversity in the I&C so that postulated I&C failures that may contribute to core damage will not preclude the operator response required for severe accident mitigation. The SAI&C supports this assumption by providing a dedicated system to support SA mitigation.

Instrumentation for monitoring of SA conditions is listed in U.S. EPR FSAR Tier 2, Table 19.2-3. Systems that may be actuated by the operator in the Level 2 PRA include:

- Primary depressurization system (PDS).
- Pressurizer safety relief valves (PSRV) (backup for PDS).
- Severe accident heat removal system (SAHRS) and cooling chain (CCWS, ESWS).
- CIS.
- Low head safety injection (LHSI).
- MFW or EFW (for steam generator tube rupture (SGTR) source term scrubbing).

The PRA does not make a specific assumption about which of these functions is available via SAI&C. The I&C functions used for SA mitigation will be provided by SAI&C, operational I&C (PAS and process information and control system (PICS)), and/or safety-related I&C (PS, SAS, and safety information and control system (SICS)). The PRA assumes that manual actuation of the functions needed for SA mitigation can be achieved via more than one I&C path so that a common cause failure (CCF) that may contribute to the SA scenario will not preclude mitigation of the SA. U.S. EPR FSAR Tier 2, Table 19.1-109, Item 45, will be revised to clarify this assumption.

#### **Response to Question 19-287, Part b:**

The dependencies between the PS and each of the other I&C systems are discussed individually in this section.

#### **PS and PAS**

The PAS is an NSR control system that is responsible for normal plant control. NSR control systems are important to the PRA because they can cause or prevent an initiating event, which is mitigated by the safety-related systems.

Normal plant control systems are typically not modeled in detail in the PRA. The reliability of these systems is important for availability of the power generation process (economic). In terms of safety, their failure represents a challenge to the safety-related systems that are responsible for reactor shutdown and event mitigation. Because the focus of the PRA model is primarily on event mitigation, the safety-related systems are modeled in more detail than the non safety-related plant control systems.



Most of the initiating events in the U.S. EPR PRA are modeled with a singular frequency that encompasses the potential causes of the initiating event. The control system contribution is not broken out separately from the other event initiator causes.

The PAS may contribute to some initiating events, and that contribution is not delineated separately in the PRA. (See the Response to Question 19-292).

The PAS impacts event mitigation. As indicated in Part a, there are a few NSR PAS functions that the PRA credits in the post-trip response. Examination of the cut sets indicates the following scenarios where the PS and PAS appear in the same cut set:

- For transients, SGTR, or a small loss of coolant accident (LOCA), the PAS-controlled SSS pump is credited before challenging the PS-actuated EFW. In the case of a loss of MFW transient, a dependency factor (0.2) was assessed between the initiating event and loss of SSS.
- For transients that affect RCP seal cooling (loss of CCWS, loss of divisional emergency AC power, Safeguard Building fire, Safeguard Building flood, and EFW pipe break flood), the PAS functions credited to prevent RCP seal LOCA (RCP protective trip and actuation of SSSS) may fail, leading to a subsequent challenge of the PS (SIS actuation).
- Anticipated transients without scram (ATWS) sequences have PS and PAS failure because the diverse actuation system (DAS) (RT function only) is modeled as a subsystem of PAS. A subsequent design change has separated the DAS from the PAS, and the DAS will be a stand alone system. This change will be incorporated into the PRA in accordance with the PRA maintenance and upgrade process described in U.S. EPR FSAR Tier 2, Section 19.1.2.4.

Due to the low truncation limits used in the quantification (see U.S. EPR FSAR Tier 2, Section 19.1.4.1.1.6), it is unlikely that there are any truncated scenarios with independent PS and PAS failures that would be significant, even if a dependency is assumed.

U.S. EPR FSAR Tier 2, Table 109, Item 46 will be revised to clarify the function of the PAS and the DAS as modeled in the PRA.

### **PS and SAS**

Both the PS and the SAS are safety-related systems that utilize the TELEPERM XS (TXS) platform, and each has four independent channels. The configuration and function of the two systems is different. The SAS provides control of safety-related systems after they have been actuated by the PS. The SAS is not a backup for the PS, and it does not provide functions that are redundant to the PS.

A search of the cut sets in the PRA found that there are no cut sets that include both failure of the PS and the SAS. There may be some scenarios that fall below the truncation limit, where SAS and PS failures of dissimilar functions could appear in the same cut set. Due to the low truncation limits used in the quantification (see U.S. EPR FSAR Tier 2, Section 19.1.4.1.1.6), it is unlikely that there are any truncated scenarios with independent PS and SAS failures that would be significant, even if a dependency is assumed.

There may be manual actions that the PRA does not credit that the operators can implement via the SAS, which may be used in the event of PS failure.

### **PS and SAI&C**

The SAI&C system is not explicitly modeled, and the PRA does not include any scenarios that specifically contain failure of the SAI&C system.

### **Response to Question 19-287, Part c:**

### **PS and PAS**

A CCF between the PS and the PAS is not expected and is not modeled. PAS failures will not impact the PS because the systems have a different purpose and safety class, and are built using different I&C platforms.

The U.S. EPR safety-related I&C systems are designed using the relevant nuclear IEEE standards (i.e., 603, 379, 3.84, 344, and 323). The TXS operating system (OS) software is developed to IEC-60880 standards and was accepted as equivalent to U.S. nuclear standards by NRC in the safety evaluation report for the TXS Topical Report, EMF-2100(NP)(A). The TXS application software is developed to U.S. nuclear standards, including IEEE 7-4.3.2, 828, 829, 830, 1012, and 1074. The TXS technology is used for the PS and SAS in the U.S. EPR design.

The PAS will use industrial technology, which is developed to different standards (e.g., IEC-62138). The difference results in the following general dissimilarities from TXS technology:

- Different network protocols.
- Different diagnostics concept.
- Different maintenance concept.
- Different hardware/operating systems for service units (SUs).
- Different HMI.
- Different signal message format and content.
- Different connectivity to external systems.
- Different information-technology (IT) security concepts.

As a result, the following diversity elements (taken from NUREG/CR-6303) distinguish the two technologies:

- Design diversity (different approaches within a technology and different architectures).
- Equipment diversity (different manufacturers of fundamentally different equipment designs).
- Functional diversity (different purpose, function, control logic, or actuation means, and different response time scale).
- Human diversity (different designers, engineers, and/or programmers).
- Signal diversity (different sensors, or the same sensors used for fundamentally different purposes).

- Software diversity (different algorithms, logic, and program architecture, different timing or order of execution, different runtime environments, and different functional representations).

### **PS and SAS**

CCF between the PS and SAS is not important to the PRA because the two systems have different functions and do not contribute to the same cut sets. A CCF is modeled between the four independent SAS channels, as indicated in the Response to RAI 138, Question 19-259.

A postulated CCF in the PS is not expected to affect other I&C systems that use the TXS platform, such as the SAS, because the TXS is designed with specific features to prevent a CCF of the platform. These features are explained in Topical Report ANP-10304, Revision 1, and are summarized as follows:

- Cyclic, deterministic, asynchronous operation.
- Interference-free communications.
- Independence of the TXS platform operation (including both hardware and system software) from the application software program.
- Fault tolerance.
- Equipment and system software qualification.
- The use of a standard library of application function blocks with operating experience.

In addition, the SAS exhibits several diversity attributes relative to the PS:

- Design (architecture) diversity.
- Functional diversity.
- Signal diversity.
- Software (algorithm and logic) diversity.

### **FSAR Impact:**

U.S. EPR FSAR Tier 2, Table 19.1-109, Item 45 will be revised as described in the response and indicated on the enclosed markup.

**Question 19-292:**

(Follow-up to Question 19-203) The response to Question 19-203 states that the general transient (GT) initiating event includes spurious actuation of the PS. How are I&C failures (e.g., software CCF) that could both cause an initiating event and affect mitigation considered in the PRA?

**Response to Question 19-292:**

Instrumentation and controls (I&C) systems that can both cause an initiating event and affect mitigation include the protection system (PS), the process automation system (PAS), and the diverse actuation system (DAS).

**PAS**

As discussed in the Response to Question 19-287, the PAS is the non-safety-related (NSR) system for normal plant control. It can cause (or prevent) an initiating event, but has minimal post-accident mitigation function.

The control system contribution to initiating event frequency is not broken out separately from the other initiating event causes. Instead, the control system contribution is subsumed in the initiating event frequencies. This is conservative because the initiating event frequencies are based on historic operating experience, and do not credit the expected improvement in initiating event frequency that the digital control system is designed to provide over the conventional I&C systems reflected in the operating experience.

Because the PAS is a distributed control system, its functions will be allocated to different computers (subsystems and divisions) to minimize the effect of individual computer failures and reduce initiating events. The purpose of the distributed control is to improve power generation availability and minimize safety-related system challenges. PAS-caused initiating events will be infrequent, and when they do occur they are unlikely to involve widespread loss of other PAS functions.

Specific details of the design of the PAS will be developed later in the design process, and it is not modeled in detail in the PRA for design certification. A sensitivity analysis is provided to conservatively estimate the impact of a potential PAS initiating event dependency. In the sensitivity analysis, the failure probability for the PAS undeveloped basic event is changed from the current value (1E-3) to 0.1. This introduces a conservative conditional probability, to encompass the possibility, given an initiating event, that PAS failure is both the cause of the initiating event, and also fails any other PAS functions credited during plant response. This is in addition (cumulative) to the 0.2 split fraction already assigned to PAS failure for loss of main feedwater (MFW) initiating events. The result of the sensitivity study is shown in Table 19-292-1.

The sensitivity study shows that there is an increase in risk when the post-trip PAS functions are not fully credited. This is mainly due to not having the full benefits of automatic actuation of the standstill seal system (SSSS) for prevention of reactor coolant pump (RCP) seal loss of coolant accident (LOCA), as well as the NSR startup and shutdown system feedwater pump. While the impact of these PAS functions is noticeable when conservative values are used, the sensitivity

study shows that the NSR functions provided by PAS are not essential to achieving acceptable risk.

As indicated in U.S. EPR FSAR Tier 2, Table 19.1-109, the PRA uses a simplified PAS model because the detailed design of PAS will occur later in the design process. The PRA model for credited PAS functions will be developed in parallel with the increasing detail of the design during the detailed design phase, including assessment of initiating event dependencies if necessary. Changes will be incorporated into the PRA in accordance with the PRA maintenance and upgrade process described in U.S. EPR FSAR Tier 2, Section 19.1.2.4.

## **DAS**

The DAS can cause an initiating event via spurious actuation. Specific details of the design of the DAS will be developed later in the design process, and are not modeled in detail in the PRA for design certification. The DAS is not included in the PRA except for a simplified model of the function that provides diverse reactor trip (RT). Because the diverse ESF actuations of DAS are not currently credited in the PRA, there is no dependency to resolve.

## **PS**

Spurious trip of the PS can cause an initiating event. The PS contribution to initiating event frequency is subsumed in the GT initiating event frequency. The frequency of initiating events caused by the PS is not broken out separately from the other initiating event causes. PS common cause failures (CCF) that can cause both an initiating event (e.g., spurious RT) and affect mitigation are not modeled.

There are no random (independent) failures that can cause a spurious PS action. To cause a spurious PS action requires an active failure (i.e., erroneous signal) in at least two independent computers (different channels) or a safe-mode failure (e.g., no signal) in at least three computers. At least as many failures are required to defeat any given ESF function. The postulated event can only be caused by a CCF.

The most plausible scenario for this to occur is a simultaneous halt (lockup or similar failure mode) in several redundant computers of different divisions. The computer failure modes associated with zero or no output are appropriate for this discussion because the safe-mode (i.e., de-energized state) for reactor protection functions corresponds to RT, and the safe-mode for ESF functions corresponds to no actuation. This hypothetical CCF mode (if it involved certain specific combinations of computers) could result in an RT and no corresponding ESF actuation.

As discussed in the Response to Question 19-284, the PS computers in redundant channels are independent and asynchronous, and are specifically designed to preclude coordinated failures in several channels simultaneously, or propagation of a failure from one computer to another. The suggested failure mode (simultaneous halt or lockup of multiple computers) is non-mechanistic. There are no identified mechanisms for this CCF in the TELEPERM XS (TXS) system (excluding supply power CCFs, which the PRA models explicitly). While the assumption of this failure in deterministic space for defining diversity-and-defense-in-depth (D3) requirements is prudent, there is no basis for an equivalent failure mode in PRA space.

Even if an improbable failure is postulated (halt of three or more redundant PS computers), core damage is unlikely. This would not lead to core damage unless there were additional failures in the systems not associated with the PS. Additional failures required for core damage include loss of MFW/startup and shutdown system (SSS) and failure of operator action (e.g., initiation of feed and bleed).

A sensitivity run was performed to show the conditional core damage probability (CCDP) that would be applicable given a postulated PS failure that resulted in a spurious RT and dependent failure of the other PS (i.e., ESF actuation) functions. In this sensitivity case, the GT event tree was quantified, with a guaranteed RT and guaranteed failure of the other PS functions. The results of the sensitivity run are shown in Table 19-292-2.

This sensitivity run indicates a CCDP of  $1.8E-3$ . This CCDP does not include the benefit of the diverse ESF actuation functions that will be implemented in DAS to address potential CCF of the PS.

Determining the contribution to core damage frequency (CDF) of the postulated scenario, requires an estimate of the frequency of the initiating event involving CCF of multiple PS computer processors. This is estimated using the combined failure rates for CCF of the computer processors and their operating systems (discussed in the Response to RAI 227, Question 19-293 (Supplement 4) and Question 19-284, respectively). There have been zero operating system (OS) failures in the field experience (92 million hours through 2008), and the OS CCF rate [ ] was derived from a chi-squared distribution with a 95 percent confidence limit, and a beta-factor of 1.0. The processor hardware has not experienced any CCF, and so a beta factor ( $5E-3$ ) was applied to the processor failure rate [ ] to obtain the processor CCF rate [ ]. This produces an estimate of the initiating event frequency for the postulated PS CCF of approximately  $5.6E-4$  per year [ ]. The postulated CCF is conservatively assumed to map to the specific combinations of three or more computer processors (of the 48 processors in the PS PRA model) that have the postulated effect.

When this initiating event frequency is combined with the calculated CCDP, the estimated CDF for this scenario is  $1.04E-6$  per year.

This result shows sensitivity to the modeling of initiating event dependencies caused by postulated CCF of the PS. This result is conservative (based on extensive operating experience and zero evidence of CCF). This result does not take credit for the diverse ESF actuation functions provided by the DAS and/or the associated operator actions, which may be required to conform with the D3 guidance of NUREG-0800, BTP 7-19. When incorporated, the DAS will reduce the uncertainty associated with this modeling, and the sensitivity of the PRA results to that uncertainty.

**FSAR Impact:**

The U.S. EPR FSAR will not be changed as a result of this question.

**Table 19-292-1—Results of Sensitivity Cases for Digital I&C: PAS dependency**

Mode	Sensitivity Case Description	CDF (1/year)
At Power	Base Case	5.26E-07
At Power	PAS = 0.1	2.14E-06
Shutdown	Base Case – Shutdown	5.77E-08
Shutdown	PAS = 0.1	3.63E-07

**Table 19-292-2—Results of Sensitivity Cases for Digital I&C: Protection System Initiating Event Dependency**

Mode	Sensitivity Case Description	IE Frequency (1/year)	CDF (1/year)	CCDP (CDF/IE Freq)
At Power	PS CCF initiating event (IE) dependency: General Transient (GT) event tree with failed PS - Reactor Trip is guaranteed success; all other PS functions guaranteed failure. Replace IE event frequency with estimated IE frequency for CCF of the PS.	5.6E-04	1.04E-06	1.85E-03

# U.S. EPR Final Safety Analysis Report Markups



### Modeling of Digital I&C Systems

Because the digital I&C system for the U.S. EPR is somewhat unique relative to systems in current plants, additional discussion of the modeling in the PRA is provided here. This addresses the manner in which system faults are reflected in the models; the sources of reliability data used; and the treatment of common-cause failures, both of software and of hardware.

Of the various I&C systems, the PS is the most important to the PRA and is modeled in detail. The PS functions include automatic initiation of reactor trip and actuation of engineered safety features (ESF).

There are other I&C systems that are not modeled in detail in the PRA. This includes the SAS, which controls certain safety-related support systems, such as CCW and ventilation, and the PAS, which controls non-safety-related systems, and also

~~performs some backup reactor trips for ATWS mitigation.~~ For the SAS and PAS, simple, high-level models and conservative failure rates are used in the PRA (i.e., undeveloped events) for design certification. ~~In order to~~ To capture dependencies, the undeveloped events for SAS and PAS are combined with power supplies and sensor inputs ~~which that~~ that could be shared with the PS.

19-284 →

Another I&C system that is modeled with an undeveloped event is the reactor trip function of the diverse actuation system (DAS), which performs some backup reactor trips for ATWS mitigation. The PAS/DAS may also contains some backup functions for ESF actuation that are being evaluated/included in the design for diversity and defense in depth (D3). These functions, which involve implementation using technology that is diverse from the PS, may/will provide additional reliability and diversity for ESF functions that is not included in the current PRA model. The D3 functions are described in Technical Report ANP-10304 (Reference 58) and in Section 7.8 but will be incorporated during detailed design if appropriate.

The PS has four-division redundancy, which contributes to its high reliability. Each of the four PS divisions is further separated into two independent subsystems to allow implementation of functional diversity. For initiating events that require reactor trip, ~~there is a primary trip signal and a diverse backup trip signals are assigned to in~~ opposite subsystems. For ESF actuation, the functions (e.g., EFW and SIS actuation) are distributed into the two subsystems, and this also provides a measure of functional diversity that increases the system reliability.

The PS is modeled to the level of detail of the rack mounted TELEPERM XS (TXS) modules. This level of detail is sufficient to resolve dependencies related to shared equipment (e.g., computer processors and I/O modules that perform multiple functions) and also corresponds to the availability of failure data from the worldwide TXS operating experience. Key PS components include computer-processor modules,

19-284 → I/O modules, signal-conditioning modules, communication modules, AV42 priority modules, subracks and power supplies, and a multitude of sensors.

The failure rates for the TXS components are derived from operating history. The TXS system is a proven design with over 10 years of operating history in reactor protection systems (RPS) and ESF actuation systems (ESFAS) in various European plants. The failure rates for the TXS components are obtained from field data and are calculated using the chi-squared distribution with a 95 percent confidence interval, and are also compared against theoretical (e.g., part stress) estimates. Due to the conservative statistical treatment inherent in the chi-squared distribution, the calculated failure rates used in the PRA are conservative relative to the observed experience. The field data for the TXS components are updated on a periodic basis.

The TXS hardware and software used by the PS have extensive self-testing features and fault-tolerant design. These features improve the reliability of the system, and minimize the need for periodic surveillance testing. However, the PRA model assumes that a portion of the failure modes are not “covered” by the self-testing and fault tolerance. With input from manufacturers analysis, the PRA model separates these failure modes and uses the failure rate equations built into the RiskSpectrum® PRA software to calculate separate component basic event unavailability for the self-revealed and test-revealed portions. The “non-covered” failure modes, although they present the smaller percentage, are more important to the PRA results, because they have a long mean time to repair (MTTR) relative to the self-revealed failures and a less favorable impact on the (fault tolerant) coincidence logic.

The PS PRA model includes two categories of software common cause failure (SWCCF): CCF of the TXS operating system (OS) software, and CCF of the application software.

19-284 → The OS CCF includes software that is common to the system including the OS itself and support software such as functional blocks. CCF of the OS is a hypothetical failure that is assumed to cause catastrophic failure of all of the PS computers. The application software CCF includes failures related to application-specific defects in functional specifications, analytical knowledge, or implementation. CCF of the application software is assumed to effect software functions or groups of related software functions that are common to redundant computer processors and share identical algorithms, sensor inputs, and signal trajectories.

Since there is uncertainty in SWCCF estimates, it is important to understand the design features that influence it. The OS design and the application software development are both significant parts of the TXS platform’s defense against CCF. The quality of the software development life-cycle process is significant in preventing defects in the application software. TXS is a mature safety I&C platform with a well-structured and controlled application software development process. The TXS platform design includes software development tools to automate application software development and reduce the likelihood of human error. A verification and validation

19-284 →

(V&V) process demonstrates that application program functional requirements are complete and correct, and that they are correctly implemented. There are also configuration control requirements for modification of the software after its initial installation.

Also significant for reducing SWCCF are the features of the OS software that reduce failure triggers. For example, application software defects can be triggered by unanticipated signal trajectories or data sets. Deterministic program execution and strictly cyclic processing are used in the TXS platform so there is only one path through the software instructions, and all of the application code is executed every cycle (i.e., the program always performs the same computations). Cyclic processing is executed with no process-driven interrupts, no real-time clock, no dynamic memory allocation, and strict measures against software exceptions (e.g., input data range violations and not-a-number violations). This provides software execution on each processor that is independent of any input data trajectory or data-triggered interference (processor overload or software exception). These characteristics of the TXS design limit the opportunity for CCF due to untested software paths and data sets, and reduce the probability that postulated latent errors may be triggered to cause failure.

~~The OS is very reliable and is supported by the mature operating history of the TXS platform. The OS design is also important for its capability to limit the impact of application SW failures, and prevent propagation of failures to redundant or diverse processing units.~~ It is a fundamental objective of the OS design, that unanticipated application software failures would not cause failure of the OS, and, therefore, propagate to other functions. This is accomplished via features such as static memory allocation and asynchronous operation. These and other features provide separation between system software and application software and eliminate leading OS failure causes in the operating history of standard computer systems, namely such as failures due to memory conflicts and failures in releasing system resources.

Another leading cause of failure that plagues standard computer systems occurs when "special loading" overtaxes the OS capacity. These failures are eliminated in the TXS platform by constant bus loading (i.e., communication and processing buses). An important consequence of by TXS features such as deterministic program execution, and strictly cyclic operation is that and constant the bus loading is constant by design and is unaffected by demands for system response (i.e., communication and processing buses). Unlike analog protection systems that sit in standby until demanded, the cyclic OS is always active, cycling many times per second, and always processing the same amount of data whether there is a demand or not. Consequently an actual system demand is no more stressful to the OS than any other cycle. ~~Deterministic program execution means that there is only one path through the software instructions, and all of the application code is executed every cycle. Primary reasons for the use of deterministic program execution and cyclic operation in the TXS platform are to~~

19-284 →

disconnect the OS from the signal trajectories and limit the opportunity for CCF due to untested software paths and data sets.

These features and others are discussed in EMF-2110(NP)(A) (Reference 54) (see also Section 7.1.1.2.1). As discussed in Reference 54, the TXS design features force a dissociation of the OS both from the application software and from external plant transients, which protects against event- or environment-related failure triggers of the OS software. This is significant with respect to the quantification of OS failure probability because it removes application-specific variability and demand-related stress from the OS reliability, and allows the OS portion of the failure probability to be calculated based upon the previous operating history.

The TXS operating history attests to the success of these features, and is used to generate a bounding value for the OS SWCCF probability. TXS I&C systems have been installed in 39 units at 24 plant sites located in 11 countries and utilizing 10 different reactor designs. TXS has broad operating experience in representative nuclear power plant applications directly applicable for use in the U.S. EPR design.

The computer processor modules have over 92 million operating hours of accumulated experience through calendar year 2008. During this time, there were some random failures of the computer processor modules, and no OS failures. A Chi-squared distribution with 95% confidence level was used to provide an upper bound OS failure rate (which at the time of analysis was based on experience through 2006). The PRA makes the conservative assumption that the failure rate of a single OS represents a CCF of the computer processors in the PS system (i.e., beta-factor = 1.0). If there was a postulated OS CCF in the field (i.e., lockup of multiple computer processors in redundant channels), a Technical Specification LCO would be triggered with a short completion time (i.e., one hour). Allowing one hour for the downtime yields an unavailability that was rounded off to 1E-7 for use as the OS CCF probability.

For the application software, the CCF probabilities are assigned based upon subjective estimates. These are based on comparison of the software development life cycle process and the TXS platform design characteristics with applicable international standards for digital systems of similar safety importance. Subjective estimates are necessary because the software is application specific. In TXS, software customization is restricted to using only qualified software functional blocks from a controlled library. The function blocks represent easily understood functions, which are thoroughly verified and tested. The medium for communication of application-specific functional specifications are functional diagrams that are composed of these function blocks. The application software designer has no access to the programming within the functional blocks, and numeric and logical operations on signals are only performed within the function block modules. The function block diagram is readily understood by both the process engineers and the I&C engineers responsible for the application software. Since the same function blocks are used and tested in many applications.

there is high confidence that they are error free. Nonetheless, the possibility of human error in specification, analytical knowledge or implementation cannot be eliminated, and it is difficult to quantify.

Therefore, the estimates for application software CCF are based on comparison of the TXS platform design characteristics and lifecycle processes for application software development with applicable international standards for digital systems of similar safety importance. The TXS design and processes are comparable to IEC-62340 (Reference 55) standards of good practice for defense against CCF, to IEC-60880 (Reference 56) standards of good practice for software, and to IEC-61508 (Reference 57) standards of good practice for safety integrity level four (SIL-4).

Reference 57 defines safety integrity level (SIL) as a relative level of risk reduction, which is assigned based on requirements in two broad categories: hardware safety integrity and systemic safety integrity (i.e., software). The TXS platform and RPS/ESFAS applications on TXS are qualified to a rigorous SIL, which is SIL-4. Reference 57 also provides risk targets, which for a SIL-4 system correspond to a failure probability between  $1E-4$  and  $1E-5$  per demand. The risk target values were used as a general guide to assign a reasonable application software failure probability based on engineering judgment. Since the target values apply to the combined hardware and the software system, engineering judgment was used to allocate half of the target range (between  $5E-5$  and  $5E-6$ ) to the software. Within this range, a value of  $1E-5$  was chosen for the application software failure probability in each of the diversity groups. The PRA makes the conservative assumption of complete dependence between redundant channels of identical application software.

19-284 →

~~Therefore, the~~ defense against application software CCF relies not only on the quality of the software development life-cycle and an OS design that prevents failure triggers and propagation, but also upon functional diversity and OS defenses to prevent propagation of failures.

Functional diversity (such as provided by the A and B subsystems for reactor trip functions) protects against application software defects. The functions assigned to the two diversity groups have different functional specifications, different sensed parameters, and different signal trajectories. Reference 55 endorses functional diversity as an effective defense against application-specific software faults such as specification errors. By introducing different signal trajectories, function diversity also protects against common failure triggers.

In terms of the SWCCF in the PRA, the application software CCF probability addresses the vulnerability introduced in the application-specific input, such as functional diagrams and specifications. The OS CCF probability addresses potential vulnerability in the OS, function block programming, or other system software that is common to both diversity groups.

19-284 →

Additional diversity is provided by other I&C systems, and human diversity is provided by the operator. The complete diversity strategy employed by the U.S. EPR I&C design is described in Chapter 7. These multiple levels of defense are beneficial to the PRA, because they will reduce the significance of the uncertainty in the SWCCF estimates.

However, the PRA does not include credit for diverse automatic or manual actuations that may be required for D3, other than diverse reactor trip (for the ATWS rule). The D3 functions are backup automatic and manual actuations that are intended to mitigate SWCCF. In order to conservatively compensate for the effect of the D3 functions that have not been incorporated into the PRA, a recovery probability of 0.5 was applied to the application software CCF probability. When fully incorporated, the D3 functions will reduce the uncertainty associated with modeling of SWCCF, and the sensitivity of the PRA results to that uncertainty.

Hardware components of the PS are also assigned to CCF groups. CCF grouping is applied to the computer hardware, to reactor trip devices (i.e., breakers, contactors), and to the PS sensor inputs. CCF for hardware devices is generally modeled using the Beta Factor or MGL method.

A CCF probability is also included for mechanical failure of control rods. The probability for stuck control rod CCF is obtained from NUREG/CR-5500, Vol. 11, Reliability Study: Babcock & Wilcox Reactor Protection System (Reference 18). Reference 18 provides estimates for the control rod CCF probabilities for the existing PWR fleet. The B&W version of this report was used because, of the three PWR vendors, the B&W design most closely resembles the EPR in terms of total number of control rods and success criteria. The B&W design has a total of 69 identical control rods of which 61 trip and 41 are considered safety-related. The NUREG/CR-5500 calculates a probability of  $4.1E-08$ /demand that 50 percent of the safety-related rods fail to insert, which corresponds to a CCF of approximately 20 rods. The U.S. EPR has 89 control rods, and analysis has shown that at least 38 control rods must fail to insert during a reactor trip before there is insufficient (less than one percent) shutdown margin. Therefore, the CCF probability from NUREG/CR-5500 is conservative for the U.S. EPR.

Fault tree top events for the ESF actuation signals are developed on a train and function-specific basis. This allows the PS fault trees to be linked with the frontline system fault trees at the train or component level of the system. In this way, the fault tree quantification resolves the hardware and software dependencies and properly accounts for the divisional redundancy and subsystem functional diversity. Key ESF functions include EFW actuation on low SG level, actuation of safety injection and PCD on low RCS (pressurizer) pressure, main steam isolation on low SG pressure, containment isolation on high pressure, and EDG starting and loading.

Fault trees for failure of the reactor trip function are developed for representative initiating events. Reactor trip fault trees specific to every initiating event are not developed because of the low probability associated with ATWS, and the extensive redundancy and diversity built into the U.S. EPR reactor trip design. ATWS is unlikely in this plant because of the diversity of reactor trip signals, the diversity in the reactor trip devices, and the abundance of control rods. Instead, representative reactor trips are modeled with a typical set of challenged parameters. This assumption is based on the PS being designed so that each postulated initiating event will challenge at least two different measured parameters for reactor trip that are implemented in the two PS subsystems. This is conservative because often there will be additional trips that the PRA could credit if the trips that are credited in the safety analysis were to fail. The representative reactor trip signals in the model include the most common trips (RCS pressure, SG pressure, SG level) as well as one of the more complex trips (low departure from nucleate boiling ratio).

As would be expected, the PS contribution to the PRA results is dominated by CCFs. The results are sensitive to the assumptions made for SWCCF, as well as CCF of

19-284 →

computers and key sensors. These sensitivities will be tempered somewhat ~~in detailed design~~ by additional functions, ~~automatic and/or manual~~, which ~~may be~~ incorporated into the PASDAS for D3, and are not credited in ~~this the design~~ certification PRA phase.

### Modeling of System Dependencies

This section provides an overview of some of the important system dependencies accounted for in the PRA of the U.S. EPR. In most cases the U.S. EPR dependencies are as expected (e.g., Division 1 of the EFW system relies on Division 1 of alternating current and direct current power) and these dependencies are not discussed in this section. Rather, this section focuses on dependencies that are either unique to the U.S. EPR design, or are non-intuitive in nature. This focus provides further background for reviewing and understanding the accident sequence results. The discussion focuses on dependencies associated with component cooling water, ventilation for the SBs, and power supplies for specific functions.

The cooling water dependencies discussed herein are illustrated in Figure 19.1-1—Cooling Water Dependencies Modeled in the U.S. EPR PRA, the ventilation dependencies are illustrated in Figure 19.1-2—Ventilation Dependencies Modeled in the U.S. EPR PRA, and the power dependencies discussed in this section are illustrated in Figure 19.1-3—Selected Dependencies on Electric Power Modeled in the U.S. EPR PRA.

19-284 →

- Failure Rates: Uncertainty distributions were obtained from the used data source.
- Digital I&C Failure Rates: Lognormal distribution was used, an error factor of five was estimated from upper & lower confidence bounds in TXS documentation. The exception is the software CCF probabilities, which are based on limited information; for their modeling, a CNI distribution was used.
- Common Cause Parameters: Uncertainty parameters were obtained from the same source as CC factors. They were fit to lognormal distribution and only applied to the “beta” factor.
- LOOP Related Basic Events: Gamma distribution for LOOP frequency, with upper and lower bounds, was fit to various LOOP events (consequential LOOPS and LOOP in 24 hours).
- Human Error Probabilities: For pre-accident HEPs, a lognormal distribution with an error factor of 10 was used, as recommended in the ASEP method. For post-accident HEPs, a constrained non-informative prior (Beta) distribution was used, as recommended in the SPAR-H method.
- Various Parameters & Undeveloped Events: Constrained non-informative prior (Beta) distribution was used, to account for the limited state of knowledge.
- Time Related Parameters: For time-related parameters, like preventive maintenance duration (and corresponding unavailability), lognormal distribution was used, an error factor was estimated from upper and lower bounds, corresponding to upper and lower time estimates.

Modeling uncertainty was also specifically treated, but limited to three cases selected to illustrate a specific lack of modeling designs details. These cases are described below:

- CASE 1: This case is based on the uncertainty of success criteria for the number of EFW trains required to cool the plant through MSSVs. The considered spectrum of success criteria included (1) one, (2) two or (3) three out of four EFW pumps required. Each of the inputs was combined with the estimated probability of that particular success criterion. This uncertainty is modeled because in a design phase, the pump flow curve is not final.
- CASE 2: This case is based on the uncertainty of success criteria for the number of pressurizer safety valves required for a success of feed and bleed. The considered spectrum of success criteria included (1) one, (2) two or (3) three out of three required. Each of the inputs was combined with the estimated probability of that particular success criterion. This uncertainty is modeled because in a design phase, conservative assumptions are made on PSVs “bleeding” capabilities.
- CASE 3: This case is based on the uncertainty of success criteria for recovery of HVAC to SBs: electrical equipment & EFW pump rooms. The considered spectrum of success criteria included: (1) Loss of HVAC will not disable equipment, (2) Operator recovery is required in 4 hours, (3) Operator recovery is



53. ANP-10309P, Revision 0, "U.S. EPR Digital Protection System Technical Report."  
AREVA NP Inc., November 2009.
54. EMF-2110(NP)(A), Revision 1, "TELEPERM XS: A Digital Reactor Protection System."  
Siemens Power Corporation, July 2000.
55. IEC-62340, "Nuclear Power Plants – Instrumentation and Control Systems Important to Safety – Requirements to Cope with Common Cause failure (CCF)."  
Edition 1.0, International Electrotechnical Commission, 12-7-2007.
56. IEC-60880, "Nuclear Power Plants – Instrumentation and Control Systems Important to Safety – Software Aspects for Computer-Based Systems Performing Category A Functions."  
Edition 2.0, International Electrotechnical Commission, 5-9-2006.
57. IEC-61508, "Functional Safety of Electrical / Electronic / Programmable Electronic Safety-Related Systems."  
International Electrotechnical Commission.
58. ANP-10304, Revision 1, "U.S. EPR Diversity and Defense-in-Depth Assessment Technical Report."  
AREVA NP Inc., December 2009.

19-284 →

Table 19.1-109—U.S. EPR PRA General Assumptions  
Sheet 8 of 17

No.	Category <sup>1</sup>	PRA General Assumptions <sup>2</sup>
40	SYS	<p>A 100% volume per day leakage rate was used to determine the size of the containment failure above which the release for a containment isolation failure was considered “large.” The results from MAAP runs performed for the Level 2 source term analysis were examined, and this resulted in the determination that:</p> <ul style="list-style-type: none"><li>• Leakage from a 1” diameter or smaller break could be neglected, as the flow rates observed were less than 10% of the threshold value for “large” releases.</li><li>• Leakage from a single 2” diameter break would fall below the criteria for “large” release.</li><li>• Leakage from two or more 2” lines, as well as any single line greater than 2” in diameter should be considered as a “large” release.</li></ul>
41	SYS	<p>The PRA model models passive flooding valves as having two failure modes. For IRWST cooling, these valves are modeled as undeveloped basic events, “Failure to Remain Closed” with an assumed failure rate of 1.00E-04. For basemat flooding in either the active or the passive mode, these valves are modeled as basic events, “Failure to Open and Remain Open” with an assumed failure rate of 1.00E-02.</p>
42	I&C	<p>Reactor trip fault trees specific to every initiating event are not developed. Instead, representative reactor trips are modeled with a typical set of challenged parameters. This assumption is based on the protection system (PS) being designed so that each postulated initiating event will challenge at least two different measured parameters for reactor trip that are implemented in the two PS subsystems.</p>
43	I&C	<p>The I&amp;C design has measures to preclude spurious operation. The frequency of initiating events caused by spurious I&amp;C actions is not modeled explicitly and is subsumed in the reactor trip and other applicable initiating events. This is a reasonable assumption because the frequency of spurious operation of the digital I&amp;C is expected to be improved relative to the historical initiating event data base.</p>
44	I&C	<p>The signal conditioning for the PS (signal modifiers, multipliers, etc.) assumes typical arrangements because design details were unavailable.</p>
45	I&C	<p>The PICS and the SICS are assumed not to be vulnerable to common cause failures based on the diversity of the PICS and the SICS I&amp;C platforms (described in Section 7.1). <u>There is sufficient diversity in the human machine interface (HMI) and connected systems that a common cause failure (CCF) will not prevent operator response for accident mitigation or for severe accident mitigation.</u></p>

↑  
19-287



Table 19.1-109—U.S. EPR PRA General Assumptions  
Sheet 9 of 17

No.	Category <sup>1</sup>	PRA General Assumptions <sup>2</sup>
46	I&C  19-287 →	<p>The system PAS contains controls for non-safety systems, and diverse backups for reactor trip and ESFAS actuations. The diverse ESFAS actuations (automatic and/or manual) are not included in the PRA model at this time because design details were unavailable. The PRA contains simplified models of the diverse reactor trip and, where needed, the non-safety control functions, where needed. The system DAS contains diverse backups for reactor trip and ESF actuations. The PRA contains simplified models of the diverse reactor trip. The diverse ESFAS actuations automatic and/or manual are not included in the design certification PRA model.</p>
47	I&C	<p>The system SAS contains controls for post-accident safety systems. The SAS model in the PRA is simplified because design details were unavailable.</p>
48	I&C	<p>The normal plant control systems (PAS and RCSL) have features to reduce the frequency and consequence of plant transients that may challenge the safety systems. This is accomplished both by the way that the control functions are distributed within the I&amp;C system divisions and by the limitation I&amp;C functions. In as much as the PRA uses historic operating experience for the initiating event frequencies, the impact of these features is not evaluated in the PRA.</p>
49	I&C	<p>Instrument calibration errors are not evaluated for the design certification PRA. Instrumentation calibration errors will be analyzed in more detail after maintenance procedures and insights from maintenance practices are available.</p>
50	LPSD	<p>RCS level and volume are treated conservatively during the RCS level transitions in outages. For example, whenever the reactor cavity is not flooded and RCS level is not in the pressurizer, mid-loop operation is assumed. The following further summarizes this conservatism:</p> <ul style="list-style-type: none"> <li>• Whenever the pressurizer is being drained, this time is applied to mid-loop.</li> <li>• Whenever the reactor cavity is being drained after refueling, this time is applied to mid-loop.</li> <li>• When level is near the flange during RPV head removal and installation, this time is applied to mid-loop.</li> <li>• When level is increased from mid-loop to fill the cavity or pressurizer, this time is applied to midloop.</li> </ul>

Next File



Table 19.1-109—U.S. EPR PRA General Assumptions  
Sheet 17 of 17

No.	Category <sup>1</sup>	PRA General Assumptions <sup>2</sup>
84	LPSD	The RCS vents identified in state CB are not considered large enough to prevent RCS repressurization in the case of loss of cooling; therefore RCS repressurization is assumed in the time to boil calculation.
85	I&C	The principles and methods for defense against software CCF in the Protection System, including operating system features that reduce failure triggers and limit failure propagation, and lifecycle processes for application software development, (described in EMF-2110(NP)(A) and referenced in Section 7.1.1.2) are comparable to industry standards of good practice described in IEC-62340, IEC-60880, and IEC-61508 for safety integrity level four (SIL-4) applications.

Notes:

↑  
19-284

- |             |                              |
|-------------|------------------------------|
| 1. Category | Description                  |
| Model       | Modeling Assumption          |
| IE          | Initiating Event             |
| CC          | Common Cause                 |
| PM          | Preventive Maintenance       |
| HRA         | Human Reliability Analysis   |
| SYS         | System Modeling              |
| I&C         | Instrumentation and Controls |
| LPSD        | Low Power/ Shutdown Modeling |
| Flood       | Flood Analysis               |
| Fire        | Fire Analysis                |
| Seismic     | Seismic Analysis             |

2. ~~The PRA assumptions will be reevaluated as part of the PRA maintenance and update process. The PRA maintenance and upgrade process is described in Section 19.1.2.4. COL item 19.1-9 listed in Table 1.8-2—U.S. EPR Combined License Information Items is provided to confirm that assumptions used in the PRA remain valid for the as-to-be-operated plant.~~