7.8 Diverse I&C Systems

The safety instrumentation and controls (I&C) systems that execute automatic reactor trip (RT) and engineered safety feature (ESF) actuation and control functions for accident mitigation are described in Sections 7.2 and 7.3. These systems are designed to perform the required safety functions in the event of a single random failure.

The overall I&C architecture can also withstand multiple failures of the safety I&C systems. The design has sufficient diversity and defense-in-depth to tolerate the following beyond design basis events:

- An anticipated transient without scram (ATWS), which is defined as an anticipated operational occurrence (AOO) followed by a failure of the RT portion of the protection system (PS).
- An AOO or a postulated accident concurrent with a software common-cause failure (CCF) that prevents the safety I&C systems from performing their required functions.

This section describes the I&C systems and functional requirements provided to mitigate these events.

AREVA NP Topical Report ANP-10284 (Reference 1) describes the following:

- The defense-in-depth concept for the U.S. EPR.
- The design features that prevent and mitigate a software CCF of the safety I&C systems.
- A methodology to evaluate the diversity and defense-in-depth of the U.S. EPR I&C architecture to determine if the I&C system will adequately protect the health and safety of the public in the unlikely event of a CCF.

The methodology described in Reference 1 is summarized in six steps:

- Step 1 - Susceptibility analysis of safety I&C systems to CCF.
- Step 2 - Qualitative evaluation of AOOs and postulated accidents.
- Step 3 - Determine inventory of diverse controls and indications.
- Step 4 - Quantitative analyses of AOOs and postulated accidents.
- Step 5 - Human factors engineering verification and validation.
- Step 6 – Platform diversity analysis.

The results of steps 1 through 3 are summarized in Section 7.8.2.2 as part of the evaluation of NUREG/CR-6303 (Reference 2) guidelines. Steps 4 and 5 are performed

as part of the plant procedure and human factors engineering verification and validation programs. For more information on these programs see Section 13.5 and Chapter 18, respectively. Step 6 is performed as inspection as part of equipment procurement. Platform diversity requirements for the process information and control system (PICS) and the process automation system (PAS) are specified in Section 7.1.

7.8.1 Description

7.8.1.1 Systems Description

7.8.1.1.1 Safety Information and Control System

The safety information and control system (SICS) provides the ability to manually trip the reactor using a hardwired actuation path that is not affected by a software CCF of the safety I&C systems.

The SICS is described in Section 7.1.

7.8.1.1.2 Process Information and Control System

The PICS provides monitoring and control of plant safety systems via the PAS and the priority and actuator control system (PACS). The PICS is diverse from the SICS.

The PICS is described in Section 7.1.

7.8.1.1.3 Process Automation System

The PAS executes manual functions initiated from PICS and automatic functions to mitigate an ATWS or software CCF of the safety I&C systems. Two subsystems of the PAS are used for these functions: the nuclear island subsystem (NIS) and the diverse actuation subsystem (DAS). The PAS is diverse from the PS and safety automation system (SAS).

The NIS enables manual component level control of safety-related plant systems. Manual commands are initiated from the PICS, processed in the NIS, and transmitted to the PACS for signal prioritization and actuation of plant components. This path allows the actuation and control of safety systems by the operator in the event of a software CCF of the safety I&C systems. Actuator related information is displayed on the PICS.

The DAS executes the automatic RT, ESF actuation, and alarm and display functions described in Section 7.8.1.2. Sensor information is acquired by the DAS from the PS and SAS using a hardwired signal that is electrically isolated within the safety I&C systems and is not affected by a software CCF. This path is described in Section 7.1.1.6. Setpoints for these functions are set so that the PS will actuate prior to the DAS.

For RT functions, outputs from the DAS are sent to the shunt trip coils of the RT breakers, which are a diverse means of opening the breakers from the undervoltage coils which are actuated by the PS.

For ESF functions, outputs from the DAS bypass the PS and SAS and are sent directly to the PACS. This path is not affected by a software CCF of the computerized portions of the safety I&C systems. Outputs for turbine trip are sent directly to the turbine generator I&C.

The DAS has online self-testing features, which minimizes the need for bypassing the system for periodic testing. Portions of the DAS that are not tested by the self-test features shall be periodically tested to ensure the system will execute its functions. Sensors that are shared by the protection system and the DAS are periodically tested as part of the PS and are not required to be tested separately as part of the DAS periodic testing.

Alarms and indications are processed by the DAS and are sent to the PICS for display.

The PAS (including the NIS and DAS) is described in Section 7.1.

7.8.1.1.4 Priority and Actuator Control System

The PACS supports the execution of automatic and manual functions required to mitigate an ATWS and a software CCF of the safety I&C systems. The PACS is diverse in operation from the TELEPERM XS (TXS) platform used in the PS and SAS. The PACS is not used in the actuation path for the RT function.

The PACS receives commands from the PAS (either from the NIS or the DAS). The system prioritizes each actuation order and sends the proper command to the safety system components. Prioritization rules for the U.S. EPR are described in Section 7.1.

The PACS is described in detail in Section 7.1.

7.8.1.2 Functional Descriptions

The functions described in this section provide the following in the event of an ATWS or software CCF of the safety I&C systems:

- Automatic actuation of RT and selected ESF systems by the DAS.
- Alarms generated by the DAS that alert the operator to an abnormal condition.
- Indications and controls for manual actions.

Unless stated in the following sections, the design basis for the functions is described in Sections 7.2 and 7.3.

These functional requirements are categorized as risk reduction I&C functions.

7.8.1.2.1 Reactor Trip on High Neutron Flux (Power Range)

This function is provided to protect the integrity of the fuel against excessive reactivity additions.

Each division of the DAS acquires two excore power range detector (PRD) measurements from the PS. The two excore PRD measurements are taken from the top half and the bottom half of the core. The DAS calculates nuclear power using excore PRDs as described in Section 7.2.

The calculated nuclear power is compared to two different setpoints. When P2 is inhibited the lower setpoint is used, which provides protection during startup and shutdown operations. When P2 is validated the higher setpoint is used, which provides protection during power operations. If two-out-of-four calculations of the nuclear power indicate greater than the active setpoint, RT signals are generated.

There are no operating bypasses associated with this function.

The logic for this function is shown in Figure 7.8-1.

7.8.1.2.2 Reactor Trip on Low RCS Flow (Two Loops)

Each division of the DAS acquires four loop flow measurements (one per loop) from the PS and executes the functional logic described in Section 7.2.1.

7.8.1.2.3 Reactor Trip on Low-Low RCS Flow (One Loop)

Each division of the DAS acquires four loop flow measurements (one per loop) from the PS and executes the functional logic described in Section 7.2.1.

7.8.1.2.4 Reactor Trip on High Pressurizer Pressure

Each division of the DAS acquires one pressurizer pressure narrow range (NR) measurement from the PS and executes the functional logic described in Section 7.2.1.

7.8.1.2.5 Reactor Trip on Low Hot Leg Pressure

Each division of the DAS acquires one hot leg pressure wide range (WR) measurement from the PS and executes the functional logic described in Section 7.2.1.

7.8.1.2.6 Reactor Trip on Low Steam Generator Pressure

Each division of the DAS acquires four steam generator pressure measurements (one per steam generator) from the PS and executes the functional logic described in Section 7.2.1.

7.8.1.2.7 Reactor Trip on High Steam Generator Pressure

Each division of the DAS acquires four steam generator pressure measurements (one per steam generator) from the PS and executes the functional logic described in Section 7.2.1.

7.8.1.2.8 Reactor Trip on Low Steam Generator Level

Each division of the DAS acquires four steam generator level NR measurements (one per steam generator) from the PS and executes the functional logic described in Section 7.2.1.

7.8.1.2.9 Reactor Trip on Safety Injection System Actuation

This function is provided to trip the reactor when the safety injection system (SIS) is automatically actuated by the DAS.

The logic for this function is shown in Figure 7.8-2.

7.8.1.2.10 Reactor Trip on Emergency Feedwater System Actuation

This function is provided to trip the reactor when the emergency feedwater system (EFWS) is automatically actuated by the DAS.

The logic for this function is shown in Figure 7.8-3.

7.8.1.2.11 Safety Injection System Actuation

The conditions used by the DAS to actuate the SIS are:

- Low pressurizer pressure NR.

Each division of the DAS acquires one pressurizer pressure NR measurement from the PS. Each pressurizer pressure NR measurement is compared to a setpoint. If two-out-of-four measurements indicate less than the setpoint, safety injection is initiated.

When P12 is satisfied, this function is bypassed. Refer to Section 7.4.2 for a description of P12.

The logic for this function is shown in Figure 7.8-2.

7.8.1.2.12 Emergency Feedwater System Actuation

The conditions used by the DAS to actuate the EFW system are:

- Low steam generator level WR.

Each division of the DAS acquires four steam generator level WR measurements (one per steam generator) from the PS. The steam generator level NR measurements are compared to a setpoint. If two out of four level measurements in any steam generator indicates less than the setpoint, emergency feedwater is initiated for that steam generator.

When P13 is satisfied, this function is bypassed. Refer to Section 7.2 for a description of P13.

The logic for this function is shown in Figure 7.8-3.

7.8.1.2.13 Main Steam Isolation

The conditions used by the DAS to isolate the main steam system are:

- Low steam generator pressure.

Each division of the DAS acquires four steam generator pressure measurements (one per steam generator) from the PS. If two-out-of-four pressure measurements in any steam generator indicates less than the setpoint, main steam is isolated.

The logic for this function is shown in Figure 7.2-19.

7.8.1.2.14 Containment Isolation

The conditions used by the DAS to perform Stage 1 containment isolation are:

- SIS actuation.

The logic for this function is shown in Figure 7.8-4.

7.8.1.2.15 Turbine Trip

Each division of the DAS acquires RT breaker position indications from the PS and executes the logic described in Section 7.3.1.

7.8.1.2.16 Manual Actuation of Critical Safety Functions

Manual actuation of the critical safety functions described in SECY 93-087 (Reference 3) is provided. Controls of safety-related process systems from the PICS via the PAS and PACS are implemented at the component level.

- Reactivity control – the reactor can be shut down by a manual actuation of RT from the SICS. Additionally, the operator can actuate the extra boration system (EBS) or the SIS from the PICS to provide the capability of injecting borated water into the core.

- Core heat removal – once the reactor is shutdown, decay heat can be removed in a variety of ways. The preferred method of removing decay heat is provided by the turbine bypass, condensate and main feedwater systems. The EFW system and the main steam relief trains (MSRT) provide a safety-grade means of removing decay heat. In addition, decay heat may also be removed using feed and bleed of the reactor coolant system (RCS). Makeup water is provided by the SIS, EBS, or chemical volume and control system (CVCS). The bleed path is provided by the pressurizer safety valves or primary depressurization valves of the RCS. Controls for these systems are available from the PICS.

- Reactor coolant inventory – RCS inventory is maintained using the CVCS, if available. Safety-grade means of reactor coolant inventory control can be performed using the SIS or the EBS. Controls for these systems are available from the PICS.

- Containment isolation – the containment is isolated by closure of containment isolation valves from the PICS.

- Containment integrity – heat is removed from the containment by actuation of the SIS from the PICS.

Refer to Chapters 5, 6 and 10 for further information regarding these process systems.

7.8.1.2.17 Alarm on Main Control Room High Radiation

This function is provided to alert the operator of high radiation condition at the main control room (MCR) intake.

Each division of the DAS acquires one MCR intake duct radiation measurement from the PS. If any of the four radiation measurements are above the setpoint, an alarm is generated in the MCR.

7.8.1.2.18 Alarm on Rod Bottom Indication

This function is provided to alert the operator of a dropped rod.

Each division of the DAS acquires one quarter of the rod bottom signals from the PS. If any of the rod bottom signals are below the setpoint, an alarm is generated in the MCR.

7.8.1.2.19 Display of Post-Accident Monitoring Variables

This function provides the operator indications to monitor the plant following an actuation by the DAS.

Each division of the DAS acquires type A, B, and C post-accident monitoring variables from the PS and SAS. The DAS processes the information and sends it to the PICS for display. The NIS processes type D and E variables for display on PICS.

The post-accident monitoring variables are described in Section 7.5.

7.8.1.2.20 Indication and Alarm of DAS Status

For the automatic RT and ESF functions described in this section, alarms are generated and sent to the PICS to alert the operator. The PICS also displays the bypassed and inoperable status of the DAS.

7.8.2 Analysis

7.8.2.1 Regulatory Requirements

7.8.2.1.1 10 CFR 50.55a(a)(1) - Quality Standards

The safety-related portions of the SICS and the PACS meet the requirements of 10 CFR 50.55a(a)(1). See Section 7.1 for a complete description on compliance with 10 CFR 50.55a(a)(1).

7.8.2.1.2 10 CFR 50.55a(h)(3) - Safety Systems

The safety-related portion of the SICS and the PACS meet the requirements of 10 CFR 50.55a(h)(3). The PICS and PAS are non-safety-related systems and are independent from the safety I&C systems. See Section 7.1 for a complete description on compliance with 10 CFR 50.55a(h)(3).

7.8.2.1.3 10 CFR 50.62 - Requirements for Reduction of Risk from ATWS Events for Light-Water-Cooled Nuclear Power Plants

The DAS is provided for ATWS mitigation, and meets the requirements of 10 CFR 50.62. The DAS automatically initiates RT, turbine trip, and EFW on conditions indicative of an ATWS to mitigate the event. The DAS performs its function reliably based on the system design and quality assurance measures taken. The DAS is independent from the PS. See Section 7.1 and Section 7.8.1.1.3 for more information on the DAS.

7.8.2.1.4 GDC 1 - Quality Standards and Records

See Section 7.1 for a description on compliance with GDC 1.

7.8.2.1.5 GDC 13 - Instrumentation and Control

See Section 7.1 for a description on compliance with GDC 13.

7.8.2.1.6 GDC 19 - Control Room

See Section 7.1 for a description on compliance with GDC 19.

7.8.2.1.7 GDC 24 - Separation of Protection and Control Systems

The SICS and PACS meet the requirements of GDC 24. See Section 7.1 for a description on compliance with GDC 24.

7.8.2.2 Evaluation of NUREG/CR-6303 Guidelines

7.8.2.2.1 Identifying System Blocks (Guidelines 1 and 5)

The blocks are identified at the system level within the I&C architecture described in Section 7.1. Within the PS, subsystems A and B provide for functional diversity.

7.8.2.2.2 Determining Degree of Diversity (Guideline 2)

The PICS and PAS are implemented with digital I&C equipment that is diverse from the TXS platform. The PACS is implemented using non-computerized technology that is diverse from the TXS digital platform. The hardwired portions of the SICS are diverse from TXS. The equipment for the PICS, PAS, PACS and SICS is described in Section 7.1.

7.8.2.2.3 System Failure Types (Guideline 3)

Type 1 Failures

Type 1 failures are caused by a failure of the I&C that induces a plant transient requiring a protective action.

These failures are mitigated in the U.S. EPR I&C design through the use of signal selection algorithms in control systems, and redundancy, fault detection and voting in the PS.

Chapter 15 identifies control system malfunctions that result in initiating events. The DAS is provided as a diverse means of actuating RT and ESF to mitigate these events concurrent with a CCF of the PS.

Type 2 Failures

Type 2 failures are undetected failures that prevent the safety I&C systems from executing safety functions, when required.

These failures are mitigated in the U.S. EPR design through two primary methods. Functional diversity within the PS is provided to mitigate an error due to a requirement specification. Equipment diversity is provided so that the PICS, PAS, PACS and hardwired portions of the SICS are not affected by a CCF of the TXS platform.

Type 3 Failures

Type 3 failures are caused by sensors that inaccurately measure the process parameter due to effects resulting from the initiating event.

These failures are mitigated in the U.S. EPR design by implementing functional diversity for RT within the PS.

7.8.2.2.4 Echelons of Defense (Guideline 4)

Four echelons of defense are defined in Reference 2:

- Control echelon.
- Reactor trip echelon.
- Engineered safety feature actuation system (ESFAS) echelon.
- Monitoring and indication echelon.

The control echelon consists of the RCSL, PAS, and turbine-generator (TG) I&C. The RT echelon consists of the PS. The ESFAS echelon consists of the PS. The SAS performs ESF control functions. The PICS and SICS comprise the monitoring echelon.

The relationship between the echelons of defense and the U.S. EPR lines of defense are described in Reference 1.

7.8.2.2.5 Postulated Common Mode Failures in System Blocks, Use of Identical Hardware and Software Modules, Effects of Other Blocks, and Output Signals (Guidelines 6, 7, 8, 9)

Systems that are implemented with the TXS platform are assumed to fail as is during a DBE. The PICS, PAS, PACS, and hardwired portions of the SICS are not affected because of diversity. Sensors shared between the safety I&C systems and the PAS are not affected by this postulated conservative failure because of the method of isolation and acquisition described in Section 7.8.1.1.3.

7.8.2.2.6 Diversity for Anticipated Operational Occurrences and Accidents (Guidelines 10 and 11)

In accordance with the methodology described in Reference 1, a qualitative evaluation of anticipated operational occurrences and postulated accidents was performed. This evaluation reviewed the design basis events analyzed in the accident analysis assuming a software common mode failure in the PS and SAS. The evaluation is strictly qualitative and credits functions designed into the DAS, primarily for ATWS, and credits limitation functions where they are diverse from the PS. Limitation functions in the RCSL share the same platform as the PS and were also assumed to fail.

Limitation and control functions in the PAS are considered. The PS includes both the reactor trip functions and the engineered safety features actuation functions. The results of the evaluation were reviewed by a multi-disciplinary team.

7.8.2.2.7 Diversity and Dependency between Echelons of Defense (Guideline 12)

Control and Reactor Trip

The DAS performs the RT functions described in Section 7.8.1.2 using equipment diverse and independent from the PS. Sensors acquired by the DAS from the PS are electrically isolated in the PS to enable independence. The reactor can be manually tripped from the SICS using a hardwired path not affected by a software CCF of the PS. Diversity in RT devices is described in Reference 1.

Control and ESFAS

The DAS performs the ESF actuation functions described in Section 7.8.1.2 using equipment diverse and independent from the PS and SAS. Sensors acquired by the DAS from the PS are electrically isolated in the PS to enable independence. Plant safety systems can be actuated at the system or component level from the SICS. Plant safety systems can be actuated at the component level from the PICS.

Reactor Trip and ESFAS

The PS performs RT and ESF actuation functions on the same processors. This reduces the number of components and improves reliability. The DAS is provided as a diverse backup in the event of a software CCF that disables both the RT and ESF actuation functions of the PS.

7.8.2.2.8 Plant Monitoring and Manual Operator Actions (Guidelines 13 and 14)

The PICS provides monitoring and control of plant systems during normal operation. In the event of a loss of the PICS, the SICS is provided as diverse backup. The safety-related portions of the SICS are independent from the PICS. The SICS and PICS are described in Section 7.1.

In the event of a CCF of the safety I&C systems, the indications and controls described in Section 7.8.1.2 are provided to the operator. These indications and controls are not subject to a CCF of the safety I&C systems. Chapter 18 describes the process of human factors engineering verification and validation for manual actions.

7.8.3 References

1. ANP-10284, "U.S. EPR Instrumentation and Control Diversity and Defense-in-Depth Methodology Topical Report," AREVA NP Inc., June 2007.

2. NUREG/CR-6303, "Method for Performing Diversity and Defense-in-Depth Analysis of Reactor Protection Systems," U.S. Nuclear Regulatory Commission, December 1994.

3. SECY-93-087, "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs," U.S. Nuclear Regulatory Commission, April 1993.

Next File