7.8 Diverse I&C Systems

The safety-related 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 distributed control system (DCS) design can also withstand software common cause failure (SWCCF) that prevents the PS from performing its functions. The design has sufficient diversity and defense-in-depth to tolerate an AOO or PA concurrent with a SWCCF of PS.

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

The U.S. EPR Diversity and Defense-in-Depth Assessment Technical Report (ANP-10304) (Reference 1) describes the following:

- The defense-in-depth concept for the U.S. EPR.
- The design features that prevent and mitigate a SWCCF of the safety-related I&C systems.
- An assessment of the I&C architecture relative to each of the 14 guidelines in NUREG/CR-6303.
- The results of a plant response analysis demonstrating that the U.S. EPR satisfies applicable acceptance criteria for a postulated SWCCF of the PS concurrent with an AOO or PA.

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 and initiate system-level critical safety functions via the diverse actuation system (DAS), which is not affected by a SWCCF of the PS. The SICS is the primary human machine interface (HMI) for the DAS.

The SICS is described in Section 7.1.

7.8.1.1.2 Deleted

7.8.1.1.3 Diverse Actuation System

The DAS executes manual functions initiated from SICS and automatic functions to mitigate an ATWS or SWCCF of the PS. The DAS is diverse from the PS.

The DAS executes the automatic RT, ESF actuation, and alarm and display functions listed in Section 7.8.1.2. Sensor information is acquired by the DAS from the signal conditioning and distribution system (SCDS) using a hardwired signal that is not affected by a SWCCF. This path is described in Section 7.1.1.6. The DAS also processes the manual, system level actuation of critical safety functions as described in Section 7.8.1.2.3.

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. An output is also sent to the rod control units of the CRDCS, which are a diverse means of dropping the control rods from the reactor trip contactors which are de-energized by the PS. The DAS outputs are energized to actuate. This design is diverse from the PS outputs, which are de-energized to actuate.

For ESF actuations, outputs from the DAS are sent directly to the PACS. This path is not affected by a SWCCF of the PS. Outputs for turbine trip are sent directly to the turbine generator I&C via a hardwired connection (one per division). The TG I&C performs two-out-of-four voting logic on the turbine trip signals. See Figure 7.1-27—Turbine Trip Logic within Turbine Generator I&C for details.

The following features are implemented so that the automatic DAS functions do not interfere with PS actuations under normal circumstances and so that the PS is given the opportunity to actuate before the DAS:

- DAS setpoints are selected to provide reasonable assurance that they will be reached after a corresponding PS setpoint is reached.
- Voting logic within the DAS is such that single failures do not result in spurious actuations of the automatic DAS functions.
- Priority logic within the PACS dictates that, in the case of conflicting orders between an “OFF/CLOSE” and an “ON/OPEN” order, the “OFF/CLOSE” orders have a higher priority (Reference 5). Based on the inventory of DAS functions compared to PS functions, a spurious “ON” order from DAS will not block the PS from performing a safety function.

The DAS functions are designed so that once initiated, they proceed to completion. The DAS functions use the same techniques as the similar PS functions to satisfy this requirement. These techniques are described in Sections 7.2.2.1.6 and 7.3.2.3.4.

The design of the DAS allows for periodic testing of the diverse RT and ESF actuation functions while retaining the capability to perform the functions in response to an event requiring protective action. The DAS components required for RT and ESF actuation are tested with the reactor at power. Surveillance of the DAS consists of overlapping tests to verify performance and response time of the RT and ESF actuation functions from sensor output to actuation order. Table 7.8-1 lists the response times for the DAS actuation functions. The definitions and allocation of response times are described in Section 7.1.2.

Sensors that are shared by the PS and the DAS are tested as part of the PS and are not required to be tested separately as part of the DAS periodic testing. The conditioning, distribution, filtering, setpoint comparison, and actuation logic associated with DAS functions are tested.

The connections between the DAS outputs and the shunt trip coils are tested during power operation. One division of the DAS and one redundancy of the shunt trip coils are tested at a time to avoid spurious reactor trip. If reactor trip orders are generated during the test, the reactor trip is performed normally.

The periodic testing of the DAS is described in ANP-10315, "U.S. EPR Surveillance Testing and TELEPERM XS Self-Monitoring Technical Report (Reference 6).

Alarms and indications are processed by the DAS and are sent to the PICS (via PAS) and SICS for display. The DAS provides accurate status information to the operator in the main control room on the PICS (via PAS) and on SICS. This includes system operation status (i.e., bypass, initiate, standby, normal), power availability, and any system faults or messages pertinent to plant operation.

The DAS is further 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 SWCCF of the PS. The PACS is diverse in operation from the PS. The PACS is not used in the actuation path for the RT function.

The PACS receives actuation orders from the various I&C systems and sends the order of highest priority to the plant actuators. The priority modules in the PACS are not subject to SWCCF by virtue of 100 percent combinatorial, proof-of-design testing. The PACS (including the methodology for performing 100 percent combinatorial testing) is described in Section 7.1.

7.8.1.1.5 Signal Conditioning and Distribution System

The SCDS provides conditioned signals from the sensors and black boxes to multiple DCS subsystems for further processing. The outputs of the SCDS are hardwired and are sent independently to each system and are not affected by a SWCCF of the PS.

The SCDS is also connected directly to the SICS via hardwire for the display of certain sensor information. The display of this information is not affected by a SWCCF of the PS.

The SCDS is described in Section 7.1.

7.8.1.2 Functional Descriptions

7.8.1.2.1 Automatic DAS Functions

The following automatic DAS functions are provided to mitigate an AOO or PA concurrent with a SWCCF of the PS:

- RT on low SG pressure.
- RT on low SG level.
- RT on high SG level.
- RT on low RCS flow (two loops).
- RT on low-low RCS flow (one loop).
- RT on high neutron flux (power range).
- RT on low hot leg pressure.
- RT on high pressurizer pressure.
- Turbine trip on RT.
- EFWS actuation on low SG level.
- SIS actuation on low pressurizer pressure.
- Main steam isolation on low SG pressure.
- Containment isolation on high activity (also includes functions that cascade from containment isolation: Annulus ventilation and Safeguards Building HVAC reconfiguration)
- MFW isolation on low SG pressure.
- MFW isolation on high SG level.

- Opening of containment hydrogen mixing dampers on high containment pressure, or high containment compartments differential pressure.
- Start SBO diesels.

7.8.1.2.2 DAS Permissives

Permissive signals are used to enable, disable, or modify the operation of DAS RT and ESF functions based on plant conditions.

The state of a permissive signal is defined either as validated or inhibited:

- A validated permissive signal carries a logical value of 1.
- An inhibited permissive signal carries a logical value of 0.

There are two Permissives, D2 and D3, which are implemented in the DAS.

D2 Permissive

The D2 Permissive is intended, in normal operation, to allow the operator to reach the shutdown states without inadvertent DAS function actuation. The D2 Permissive uses the same excore power measurement devices as the Protection System P2 Permissive. The D2 Permissive is validated when the indicated power is higher than its setpoint of 10% nominal power. The validation of the D2 Permissive will follow the same two-out-of-four logics as the P2 Permissive shown in Figure 7.2-25—P2 Permissive Logic.

The D2 Permissive is automatically validated when the power increases above 10% and can be manually inhibited when the power is below the setpoint (10% power). The validation of the D2 Permissive automatically enables all of the DAS functions (RT and ESF) except the RT on Low-low Reactor Coolant System (RCS) Flow (One Loop). The inhibition of the D2 Permissive automatically disables all of the DAS functions (RT and ESF) except the RT on Low-low RCS Flow (One Loop).

D3 Permissive

The D3 Permissive is intended to prevent a full reactor trip actuation following a partial reactor trip due to the loss of one Reactor Coolant Pump (RCP) event. The D3 Permissive uses the same excore power measurement devices as the Protection System P3 Permissive. The D3 Permissive is automatically validated when the indicated power is higher its setpoint of 70% nominal power. The validation of the D3 Permissive will follow the same two-out-of-four logics as shown in Figure 7.2-26—P3 Permissive Logic.

The D3 Permissive is automatically validated when the power increases above 70% and automatically inhibited when the power decreases below 70%. The validation of the D3 Permissive automatically enables the RT on the Low-low RCS Flow (One

Loop). The inhibition of the D3 Permissive automatically disables the RT on a Low-low RCS Flow (One Loop).

7.8.1.2.3 Manual Functions

The following manual functions are provided to mitigate an AOO or PA concurrent with a SWCCF of the PS. The allocation of the function within the DCS design is provided.

- Manual RT (SICS/DAS/PACS) (Note 1).
- Manual EDG start (SICS/PACS) (Note 2).
- Manual component controls to support diesel generator loading (emergency diesel generators or SBOs) (SICS/PACS) (Note 2).
- Manual EFW actuation (SICS/DAS/PACS) (Note 1).
- Manual operation of EFW for long-term SG level control (SICS/PACS) (Note 2).
- Manual SI switchover to hot leg injection (SICS/PACS) (Note 2).
- Manual MSIV closure (SICS/PACS) (Note 2).
- Manual feedwater isolation (MFW and EFW) (SICS/PACS) (Note 2).
- Manual initiation of medium head safety injection (MHSI) (SICS/DAS/PACS) (Note 1).
- Manual control of MHSI (SICS/PACS) (Note 2).
- Manually extend partial cooldown (SICS/PACS) (Note 2).
- Manual depressurize RCS with pressurizer sprays (SICS/PACS) (Note 2).
- Manual actuation of extra borating system (EBS) (SICS/PACS) (Note 2).
- Manual control room HVAC reconfiguration (SICS/PACS) (Note 2).
- Manual CVCS isolation (SICS/PACS) (Note 2).
- Manual MSRT control (SICS/PACS) (Note 2).
- Manual Stage 1 containment isolation (SICS/DAS/PACS) (Note 1).
- Manual opening of containment hydrogen mixing dampers (SICS/DAS/PACS) (Note 1).

Notes:

1. Function is used to satisfy BTP 7-19 Point 4.

2. Manual component controls required for diversity and defense-in-depth are credited via the SICS/PACS path. In addition, manual component controls are provided via PICS/PAS/PACS path. The operator will perform these actions from PICS as long as PICS is available.

The manual functions are subject to evaluation and design per the human factors engineering program described in Chapter 18. All of the manual actions are analyzed during task analysis as described in Section 18.4.2. Furthermore, the actions are included in the overall population of human actions that are subject to task support verification and integrated system validation as described in Sections 18.10.3.1, 18.10.3.3, and 18.10.3.5.

7.8.1.2.4 Indications and Alarms

The following indications and alarms are processed by the SCDS and provided to the operator on the PICS and SICS:

- Post-Accident Monitoring Variables – The operator is provided with indications to monitor the plant following an actuation by the DAS. The SICS acquires Type A, B, and C post-accident monitoring variables from the SCDS. The SCDS processes the information and sends it to the SICS for display to the operator. Post-accident monitoring variables are described in Section 7.5.

- Indication and Alarm of DAS Status – When an automatic RT or ESF function is actuated by DAS, alarms are generated and sent to the PICS (via PAS) and SICS to alert the operator.

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, SCDS, 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, SCDS, and the PACS meet the requirements of 10 CFR 50.55a(h)(3). The DAS is a non-safety-related system and is independent from the safety-related 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, SCDS, and PACS are provided for ATWS mitigation, and meet 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 of compliance with GDC 1.

7.8.2.1.5 GDC 13 - Instrumentation and Control

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

7.8.2.1.6 GDC 19 - Control Room

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

7.8.2.1.7 GDC 24 - Separation of Protection and Control Systems

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

7.8.2.1.8 Generic Letter 85-06 - Quality Assurance Guidance for ATWS Equipment that is not Safety Related

AREVA Inc. implements quality requirements to ATWS equipment in accordance with Generic Letter 85-06, "Quality Assurance Guidance for ATWS Equipment that is not Safety Related" (Reference 4).

7.8.3 References

1. [*ANP-10304, Revision 6, "U.S. EPR Diversity and Defense-in-Depth Assessment Technical Report," AREVA NP Inc., May 2013.*]*

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.

4. Generic Letter 85-06, "Quality Assurance Guidance for ATWS Equipment That Is Not Safety-Related," U.S. Nuclear Regulatory Commission, April 16, 1986.

5. [*ANP-10310P, Revision 2, "Methodology for 100% Combinatorial Testing of the U.S. EPR Priority Module Technical Report," AREVA NP Inc., May 2013.*]*

6. *ANP-10315, Revision 2, "U.S. EPR Surveillance Testing and TELEPERM XS Self-Monitoring Technical Report."*]*

Table 7.8-1—Diverse Actuation Function Response Times
Sheet 1 of 2

Function	Total Response Time(s)	T1	T2	T3	T4	T3 Definition	T4 Definition
RT on High Pressurizer	5.3	0.4	1.0	0.25	3.65	See Note 1	See Note 2
RT on Low hot leg pressure	5.3	0.4	1.0	0.25	3.65	See Note 1	See Note 2
RT on Low SG pressure	5.3	0.4	1.0	0.25	3.65	See Note 1	See Note 2
RT on Low SG level	5.9	1.0	1.0	0.25	3.65	See Note 1	See Note 2
RT on High SG level	5.9	1.0	1.0	0.25	3.65	See Note 1	See Note 2
RT on Low RCS flow rate (2 loops)	4.8	0.4	0.5	0.25	3.65	See Note 1	See Note 2
RT on Low-low RCS flow rate (one loop)	4.8	0.4	0.5	0.25	3.65	See Note 1	See Note 2
RT on High neutron flux (PR)	4.5	negligible	0.6	0.25	3.65	See Note 1	See Note 2
SIS actuation on Low Pressurizer pressure	17.6	0.4	2.2	0.5	14.5	See Note 3	The maximum time delay for valve and pump actuation. See Note 4 for more details.
EFWS actuation on High SG Level	17.0	1.0	1.0	0.5	14.5	See Note 3	The maximum time delay for valve and pump actuation. See Note 4 for more details.
Partial Cooldown Actuation (via TBS) on Low Pressurizer pressure	None	N/A	N/A	N/A	N/A	N/A	N/A
MSIV closure on Low SG pressure	6.4	0.4	1.0	0.5	4.5	See Note 3	The maximum time delay for valve and pump actuation. See Note 4 for more details.
MFW full load isolation on High SG Level (affected SG)	42.0	1.0	1.0	0.5	39.5	See Note 3	The maximum time delay for valve and pump actuation. See Note 4 for more details.

Table 7.8-1—Diverse Actuation Function Response Times
Sheet 2 of 2

Function	Total Response Time(s)	T1	T2	T3	T4	T3 Definition	T4 Definition
MFW SSS isolation on Low SG pressure (affected SG)	21.4	0.4	1.0	0.5	19.5	See Note 3	The maximum time delay for valve and pump actuation. See Note 4 for more details.
Containment isolation on High containment activity (Stage 1)	5.5 plus T3 and T4	4.5	1.0	See Section 6.2.4	See Section 6.2.4	See Note 3	The maximum time delay for valve and pump actuation. See Note 4 for more details.
Turbine Trip on Initiation of RT	N/A (See Note 5)	N/A	N/A (See Note 5)	N/A	N/A	N/A	N/A
Hydrogen Mixing Dampers Opening on High containment service compartment pressure (NR)	18.5	0.4	1.0	0.5	16.6	See Note 3	The maximum time delay for valve and pump actuation. See Note 4 for more details.
Hydrogen Mixing Dampers Opening on High containment equipment compartment/containment service compartment ΔP	18.5	0.4	1.0	0.5	16.6	See Note 3	The maximum time delay for valve and pump actuation. See Note 4 for more details.

1. The maximum delay time for opening the RT breakers and rod control units considering the shunt trip operating time, mechanism operating time, arcing time, and auxiliary relay operating time.

2. The maximum delay time between de-energizing the holding coils and the RCCAs fully inserted (e.g., bottom position indication) (gripper release time of 0.15 sec + RCCA drop time of 3.5 sec).

3. The maximum delay time from the input of the switchgear or MCC to the input of the motors, pumps, valves, etc. considering the shunt trip operating time, mechanism operating time, arcing time, and auxiliary relay operating time.

4. The following is the T4 definition for various actuated equipment in the plant:
   For all valves (or dampers): The maximum time delay from when the valve (or damper) receives the signal from the switchgear to when the valve (or damper) goes to full open or full closed position.

   – For motor operated valves: The maximum time delay from when the motor receives the signal from the MCC to when the valve goes to full open or full closed position.

   – For air-operated valves: The maximum time delay from when the valve receives the signal from the switchgear to when the valve goes to full open or full closed position. This includes the time it takes the solenoid (air supply) or pilot valve to actuate.

   – For hydraulic actuated valves: The maximum time delay from when the valve receives the signal from the switchgear to when the valve goes to full open or full closed position. This includes the time it takes the solenoid (control flow of hydraulic fluid) or pilot valve to actuate.

   – For pumps: The maximum time delay from when the pump receives a signal from MCC or switchgear to when the pump provides full flow.

5. The response time indicated for the Turbine Trip on RT is the minimum time based on the capability of the DAS equipment. The D3 assessment requires a minimum response time of at least one second between a RT and a Turbine Trip. Therefore, a one-second time delay is implemented in the DAS software design for this function.

Next File