7.5 Information Systems Important to Safety

The information necessary to monitor the nuclear steam supply systems (NSSS), the containment systems, and the balance of plant is displayed on the operator console and the various screens and panels located within the main control room (MCR). Information systems important to safety are those systems that provide information to control and operate the unit safely through all operating conditions, including anticipated operational occurrences (AOO), accident and post-accident conditions. This section is limited to the description of those display instruments that provide information to enable the operator to assess reactor status, the onset and severity of accident conditions, and engineered safety feature (ESF) actuation status and performance, or to enable the operator to reliably perform vital manual actions such as safe shutdown and initiation of manual ESF actuation.

This section also provides information on the classification of monitored variables, which is based on the guidance provided by RG 1.97, Revision 4, which endorses IEEE Std 497-2002 (Reference 1), with certain clarifying regulatory positions. A methodology for selecting the post-accident monitoring (PAM) variables based on IEEE Std 497-2002 (Reference 1) is presented in Section 7.5.2.2.1.

7.5.1 Description

This section discusses the instrumentation and controls (I&C) used to provide information important to safety and to provide a means for manual operator action related to accident mitigation.

7.5.1.1 Annunciator Systems

The annunciator system consists of alarms and functions to enable operators to silence, acknowledge, reset, and test alarms. The non-safety-related process information and control system (PICS) is the primary annunciator system. In the event of an abnormal plant or system condition, the operator will receive an indication of the abnormal event. Icons will be displayed on the PICS screens to allow the operator to acknowledge the alarm and to view system diagrams of the affected system.

The safety information and control system (SICS) provides limited annunciation functions to support accident mitigation.

The architecture and functions of the PICS and SICS are described in Section 7.1.

7.5.1.2 Post-Accident Monitoring Instrumentation

The PAM instrumentation provides plant process variable information and system status to the operator in the MCR to permit the operator to perform the following:

- Preplanned manual safety functions.

- Capability to assess plant conditions, safety system performance, and determine appropriate actions to take to respond to abnormal events.
- Capability to bring the plant to a safe shutdown condition.

The PAM instrumentation utilizes the components of existing safety-related and non-safety-related I&C systems to accomplish PAM functions. The PAM variables are displayed on the non-safety-related PICS. Additionally, Type A, B, and C PAM variables are displayed on the safety-related SICS. The priority and actuator control system (PACS), SICS, and PICS contain the hardware to obtain and display the safety-related and non-safety-related PAM variables. The selection of PAM variables is described in Section 7.5.2.2.1.

7.5.1.3 Emergency Response Information

The description of the emergency response information capability in this section is limited to the system interface with the plant I&C systems. The safety parameter display system (SPDS), Emergency Response Data System (ERDS), and technical support center (TSC) are designed and implemented in accordance with NUREG-0696 (Reference 4), NUREG-0654 (Reference 5) and NUREG-0737 (Reference 6).

The PICS provides a means of transmitting data through a firewall to systems external to the plant I&C systems. Details of the architecture of PICS are provided in Section 7.1.

The TSC contains PICS workstations that display pertinent information for plant management and technical support personnel. These workstations do not send control signals to the PICS. The PICS provides the SPDS display.

7.5.1.4 Bypass and Inoperable Status Indication

Bypassed and inoperable status indication (BISI) of safety-related systems is provided by the PICS. BISI is also discussed in Section 7.5.2.1.1, Section 7.5.2.2.4, and Section 7.5.2.2.5.

7.5.2 Analysis

The human factors engineering (HFE) program described in Chapter 18 provides a design process that reasonably assures that plant operators can access the required information and controls to enable safe and efficient control and monitoring of plant processes and equipment. As part of the HFE program, verification and validation evaluations will confirm that the human system interfaces provide the operator with sufficient information to perform required manual safety functions and sufficient time to make reasoned judgments and take action where operator action is essential for maintaining the plant in a safe condition.

7.5.2.1 Acceptance Criteria

The following acceptance criteria guidance listed in NUREG-0800 (Reference 10), Section 7.5, apply to the I&C systems listed in Section 7.5.1.

Compliance with the following requirements is discussed in Section 7.1:

- 10 CFR 50.55a(a)(1), “Quality Standards”.
- 10 CFR 50.55a(h), “Protection and Safety Systems”.
- GDC 1, “Quality Standards and Records”.
- GDC 2, “Design Basis for Protection against Natural Phenomena”.
- GDC 4, “Environmental and Missile Design Basis”.
- GDC 19, “Control Room”.
- GDC 24, “Separation of Protection and Control Systems”.

7.5.2.1.1 10 CFR 50.34(f), “Additional TMI-Related Requirements”

The following TMI-related requirements apply:

10 CFR 50.34(f)(2)(v) Bypassed and Inoperable Status Indication

If any Type A, B, and C PAM variable is bypassed or rendered inoperable, an indication is provided to the operator in the MCR. Description of the bypassed and inoperable status of safety systems is provided in Section 7.5.2.2.4.

10 CFR 50.34(f)(2)(xi) Direct Indication of Relief and Safety Valve Indication

Three pressurizer safety relief valves (PSRV) are arranged at the top of the pressurizer (PZR) for overpressure protection of the reactor coolant system (RCS). Each PSRV is provided with a position sensor. The position (open or closed) for each valve is indicated in the MCR. The PSRVs are described in Section 5.4.13.

10 CFR 50.34(f)(2)(xii) Auxiliary Feedwater Flow Indication

Indication of emergency feedwater (EFW) flow to each steam generator (SG) is provided in the MCR. EFW flow sensors are shown in Figure 10.4.9-1.

10 CFR 50.34(f)(2)(xvii) Accident Monitoring Instrumentation

The following instrumentation is available for readout in the MCR:

- Containment pressure sensors are provided by the containment ventilation system described in Section 9.4.7.

- Level sensors for the in-containment refueling water storage tank (IRWST) are provided by the safety injection system described in Section 6.3.

- Containment hydrogen sensors are provided by the hydrogen monitoring system described in Section 6.2.5.

- Containment radiation activity (high level) monitors are provided by the containment high range monitors described in Section 12.3.4.1.3 and Table 12.3-3.

- Noble gas effluent monitoring at all potential accident release points are provided by the RMS described in Section 11.5 and Table 11.5-1.

- Continuous sampling of radioiodines and particulates from all potential accident release points is provided by the process sampling system as described in Section 11.5 and Table 11.5-1. Additional details on the process sampling system are described in Section 9.3.2.

10 CFR 50.34(f)(2)(xviii) Inadequate Core Cooling Instrumentation

The following instrumentation provides an indication in the MCR of inadequate core cooling:

- A combination of RCS hot leg wide range (WR) pressure and the core outlet thermocouples (COT) described in Section 7.1 is used to determine inadequate core cooling. In addition, the reactor vessel water level indication is provided by the reactor pressure vessel water level measurement system described in Section 7.1.

10 CFR 50.34(f)(2)(xix) Instruments for Monitoring Plant Conditions Following Core Damage

The PAM variables discussed in Section 7.5.2.2.1 and the severe accident monitoring variables discussed in Section 7.5.2.2.3 provide for monitoring plant conditions following core damage.

10 CFR 50.34(f)(2)(xx) Power for Pressurizer Level Indication

Each of the four PZR level sensors generates a signal that is received in one of the four divisions of the PS. The PZR level sensors are powered from the Class 1E bus of the PS division in which the sensor signal is received. PZR level indication is provided by both the PICS and the safety-related SICS.

Each division of the PS and the SICS is supplied by an independent Class 1E, uninterruptible electrical bus. These busses are backed by the emergency diesel generators to cope with loss of offsite power. Inside a division, the PS cabinets are supplied by two redundant, uninterruptible 24 Vdc feeds. To cope with loss of onsite and offsite power, the feeds to the PS cabinets are supplied with two-hour batteries.

7.5.2.1.2 GDC 13, "Instrumentation and Control"

The PICS and SICS provide the capability for monitoring PAM variables and system variables over their anticipated ranges for normal operation, for AOOs, and for postulated accident conditions as appropriate. This monitoring provides reasonable assurance of safety by including those variables and systems that can affect the fission process, the integrity of the reactor core, the reactor coolant pressure boundary, or the containment and its associated systems. The PICS and SICS also provide a means of manual control capabilities for maintaining these variables and systems within prescribed operating ranges.

7.5.2.2 Discussion

7.5.2.2.1 Conformance to Regulatory Guide 1.97 and BTP 7-10

With clarifying regulatory positions, RG 1.97, Revision 4, endorses IEEE Std 497-2002 (Reference 1), which provides performance-based criteria for selecting variables and recommends determining the variable type according to its accident management function. The accident management function is to be identified by its use in the Emergency Procedure Guidelines (EPG), Emergency Operating Procedures (EOP), and Abnormal Operating Procedures (AOP).

Section 13.5.2.1.2 describes the EOP development process. Preparation of EOPs and AOPs for the U.S. EPR plant requires detailed design of systems to be completed. Because preparation of procedures is not required for design certification, an alternative to the use of EOPs and AOPs in the IEEE 497-2002, Section 4.0 Selection Criteria, was performed to develop the list of PAM variables for the U.S. EPR plant. The alternative included:

- A step-by-step evaluation of Volume 1 of the AREVA Emergency Operating Procedures Technical Basis Document (Reference 11) was performed to identify required supporting instrumentation. The evaluation considered the differences in the U.S. EPR and the B&W plant designs.

- A review of the operator manual actions listed in Chapter 15 for which no automatic control is provided to determine instrumentation required to support those actions.

- A review of radiation monitoring system design to identify instruments necessary to support post-accident monitoring.

- Identification of additional instrumentation based on engineering judgment considering differences between the U.S. EPR and the B&W plant designs.

- An evaluation was performed to confirm that critical safety functions and fission product barriers described in IEEE Std 497-2002 were adequately monitored by the list of instruments developed.

The list of PAM variables is provided in Table 7.5-1.

A COL applicant that references the U.S. EPR design certification will identify the need for site-specific PAM variables.

Criteria for Selection of Variable Types

In accordance with RG 1.97, Revision 4, and IEEE Std 497-2002, the PAM variables are selected and the variable types are determined according to its accident management function. These variables are the primary source of post-accident monitoring information. Five types of variables exist and the selection criteria are described as follows:

Type A Variables

Type A variables are those variables that provide the primary information required to permit the control room operating staff to:

- Take specific pre-planned manually-controlled actions for which no automatic control is provided and that are required for safety systems to perform their safety-related functions as assumed in the plant Accident Analysis Licensing Basis.
- Take specific planned manually-controlled actions for which no automatic control is provided and that are required to mitigate the consequences of an AOO.

As recommended by RG 1.97, Revision 4, Type A variables include those variables that are associated with contingency actions that are within the plant licensing basis and may be identified in written procedures.

Type B Variables

Type B variables are those variables that provide primary information to the control room operators to assess the accomplishing or maintaining of plant critical safety functions.

Type C Variables

Type C variables are those variables that provide primary information to the control room operators of the potential for breach, or the actual breach, of the three fission product barriers (extended range): fuel cladding, reactor coolant system pressure boundary, and containment pressure boundary.

The selection of these variables represents a minimum set of plant variables that provide the most direct indication of the integrity of the three fission product barriers. They also provide the capability for monitoring beyond the normal operating range.

Type D Variables

Type D variables are those variables that are required in procedures and licensing basis documentation to:

- Indicate the performance of those safety systems and auxiliary supporting features necessary for the mitigation of design basis events (DBE).
- Indicate the performance of other systems necessary to achieve and maintain a safe shutdown condition.
- Verify safety system status.

Type D variables are based upon the plant accident analysis licensing basis and those necessary to implement the following procedures, which are applicable to the plant design:

- Event-specific EPGs or plant-specific EOPs.
- Functional restoration EPGs or plant-specific EOPs.
- Plant AOPs.

Type E Variables

Type E variables are those variables required for use in determining the magnitude of the release of radioactive materials and continually assessing such releases.

These variables are selected to:

- Monitor the magnitude of releases of radioactive materials through identified pathways.
- Monitor the environmental conditions used to determine the impact of releases of radioactive materials through identified pathways.
- Monitor radiation levels and radioactivity in the plant environs.
- Monitor radiation levels and radioactivity in the control room and selected plant areas where access may be required for plant recovery.

Post-Accident Monitoring Instrumentation Criteria

The PAM instrumentation are designed in accordance with the performance (criterion 5), design (criterion 6), qualification (criterion 7), and display criteria (criterion 8) of IEEE Std 497-2002 with the modifications specified in RG 1.97, Revision 4, and in accordance with the supplemental guidance provided in BTP 7-10 (Reference 7).

7.5.2.2.2 Use of Digital Systems

The human machine interface (HMI) systems provide the ability to control and monitor the plant operation. The HMI systems consist of the SICS and PICS. The PICS is implemented using a digital computer platform. The SICS is implemented using hardwired I&C and the qualified display system (QDS).

The QDS is an HMI that is qualified to non-safety-related supplemented grade (NS-AQ) to meet Seismic Class II criteria.

To minimize the potential for non-safety-related digital control system failures that could challenge safety systems, non-safety-related digital control system hardware and software is developed using a structured process similar to that applied to safety-related system software; however, the process is tailored to account for the lower safety significance. The hardware and software development process for PICS is described in Section 7.1.

7.5.2.2.3 Monitoring for Severe Accidents

Instrumentation used to monitor severe accident conditions are identified in Table 19.2-3. The severe accident response instrumentation is designed so there is reasonable assurance that the instrumentation will operate in the severe accident environment for which they are intended and over the time span for which they are needed.

7.5.2.2.4 Conformance to Regulatory Guide 1.47

If a protective function of some part of a safety-related system has been bypassed or deliberately rendered in-operative, continued indication of the bypassed condition is provided in the MCR.

The PS and the SAS are the safety-related system level automation systems. Both systems provide display signals to the PICS. Outputs to PICS from safety-related systems are supplied through qualified isolation devices. If the PS or SAS is operated in a bypassed mode or inoperable condition, an output is automatically provided to the PICS for indication of the bypass or inoperable condition in accordance with the guidance of RG 1.47, and Clause 5.8.3 of IEEE Std 603-1998 (Reference 3).

7.5.2.2.5 Scope of Bypassed and Inoperable Status Indications

The BISI in the MCR includes bypasses of the reactor trip (RT) functions described in Section 7.2 and ESF functions described in Section 7.3. In addition, BISI is provided for the safety injection system (SIS) accumulator isolation valves and the residual heat removal (RHR) system suction isolation valves. If any SIS accumulator isolation valve comes off its open seat during conditions that require the valve to be open, a bypass indication will be provided in the MCR. If any RHR system suction isolation valve comes off its closed seat during conditions that require the valves to be closed, a bypass indication will be provided in the MCR.

7.5.2.2.6 Redundancy and Diversity of Display

Type A, B, and C PAM variables are sent directly from the SCDS to the SICS via hardwired connections bypassing software based components. Diverse display of variables is not required. The same variables are processed through the PAS and PICS to provide a redundant path.

7.5.2.2.7 Independence and Compliance with IEEE Std 603-1998

Section 7.1 describes the overall I&C system architecture and how independence is achieved between safety-related and non-safety-related I&C systems. Compliance with Clause 5.6.3, “Independence Between Safety Systems and Other Systems,” and Clause 6.3, “Interaction Between the Sense and Command Features and Other Systems,” are addressed in Section 7.1.

7.5.3 References

1. IEEE Std 497-2002, “Standard Criteria for Accident Monitoring Instrumentation for Nuclear Power Generating Stations,” Institute of Electrical and Electronics Engineers, 2002.

2. Deleted.

3. IEEE Std 603-1998, “IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations,” Institute of Electrical and Electronics Engineers, 1998.

4. NUREG-0696, “Functional Criteria for Emergency Response Facility,” Nuclear Regulatory Commission, 1981.

5. NUREG-0654, “Criteria for Preparation and Evaluation of Radiological Emergency Response Plans and Preparedness in Support of Nuclear Power Plants,” Nuclear Regulatory Commission, 1980.

6. NUREG-0737, “Clarification of TMI Action Plan Requirements,” Nuclear Regulatory Commission, 1980.

7. NUREG-0800, BTP 7-10, “Guidance on Application of Regulatory Guide 1.97,” Nuclear Regulatory Commission, March 2007.

8. Deleted.

9. Deleted.

10. NUREG-0800, “Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants,” Nuclear Regulatory Commission, March 2007.

11. "Emergency Operating Procedures Technical Bases Document, Volume 1, Generic Emergency Operating Guidelines," Revision 10, AREVA NP Inc., December 31, 2005.

Table 7.5-1—Inventory of Post-Accident Monitoring Variables
Sheet 1 of 4

No	Variable	Range	Minimum Channels Required	Duration	Safety Class	EQ[1] per IEEE Std 323-1974	Seismic Qualification	Type				
								A	B	C	D	E
1	Annulus Ventilation System Gamma Activity	See Table 11.5-1, R-27	2	1 year	NS-AQ	Yes	I			X		X
2	Vent System for Air Removal Radiation	See Table 11.5-1, R-3	1	24 hours	NS	No	NSC					X
3	Containment High Range Radiation	See Table 12.3-3	2	1 year	S	Yes	I		X	X		X
4	Containment Isolation Valve Position Indications	Closed/not closed	1 / valve	1 year	S	Yes	I		X			
5	Containment Service Compartment Wide Range Pressure	-5 to 220 psig	2	1 year	S	Yes	I			X	X	
6	Core Outlet Thermocouples Wide Range Temperature	32 to 2300°F	8 (2 / quadrant)	1 year	S	Yes	I		X	X	X	
7	Extra Borating System Flow	0 to 60 gpm	1 / train	24 hours	S	Yes	I				X	
8	Emergency Feedwater Flow to SG	0 to 545 gpm	2 / train	24 hours	S	Yes	I	X	X		X	
9	Emergency Feedwater Wide Range Pool Level	0 to 300 inches	1 / train	24 hours	S	Yes	I				X	
10	Emergency Power Supply System Voltage	0 to 8625 VAC	1 /train	1 year	S	Yes	I				X	
11	Fuel Building Fuel Pool Dose Rate	See Table 12.3-3	1	24 hours	NS	No	NSC					X

Table 7.5-1—Inventory of Post-Accident Monitoring Variables
Sheet 2 of 4

No	Variable	Range	Minimum Channels Required	Duration	Safety Class	EQ[1] per IEEE Std 323-1974	Seismic Qualification	Type				
								A	B	C	D	E
12	Fuel Building Setdown Dose Rate	See Table 12.3-3	1	24 hours	NS	No	NSC					X
13	Hot Leg Injection Flow	0 to 3200 gpm	1 / train	1 year	S	Yes	I				X	
14	Intermediate Range Nuclear Instrumentation	5 x 10^{-6} to 60% NP	2	2 hours	S	Yes	I		X		X	
15	In-containment Refueling Water Storage Tank Level	0 to 20 feet	1	1 year	S	Yes	I				X	
16	Low Head Safety Injection Wide Range Flow	0 to 3800 gpm	2 / train	1 year	S	Yes	I		X		X	
17	Main Control Room Dose Rate	See Table 12.3-3	1	24 hours	NS	No	NSC					X
18	Main Steam Line Radiation	See Table 11.5-1, R-55 through R-58	2 / line	2 hours	S	Yes	I	X	X			
19	Medium Head Safety Injection Wide Range Flow	0 to 1300 gpm	2 / train	24 hours	S	Yes	I		X		X	
20	Pressurizer Level	0 to 100%	2	24 hours	S	Yes	I	X	X			
21	Pressurizer Safety Relief Valve Position Indication	Closed/not closed	1 / valve	24 hours	NS-AQ	Yes	I				X	
22	Reactor Coolant System Hot Leg Pressure	0 to 3000 psig	2	1 year	S	Yes	I	X	X	X		
23	Reactor Coolant System Wide Range Cold Leg Temperature	32 to 662 °F	2	24 hours	S	Yes	I	X	X		X	

Table 7.5-1—Inventory of Post-Accident Monitoring Variables
Sheet 3 of 4

No	Variable	Range	Minimum Channels Required	Duration	Safety Class	EQ[1] per IEEE Std 323-1974	Seismic Qualification	Type A	Type B	Type C	Type D	Type E
24	Reactor Coolant System Wide Range Hot Leg Temperature	32 to 662 °F	2	24 hours	S	Yes	I	X				
25	Reactor Building Personnel Air Lock Dose Rate	See Table 12.3-3	1	24 hours	NS	No	NSC					X
26	Safeguard Building Controlled-Area Ventilation System Gamma Activity	See Table 11.5-1, R-26	1	1 year	NS-AQ	Yes	II					X
27	Safeguard Building Corridor Dose Rate	See Table 12.3-3	1 / building	24 hours	NS	No	NSC					X
28	Safeguard Building Personnel Air Lock Dose Rate	See Table 12.3-3	1	24 hours	NS	No	NSC					X
29	Steam Generator Pressure	0 to 1600 psig	2 / SG	24 hours	S	Yes	I	X	X		X	
30	Steam Generator Wide Range Level	0 to 100%	2 / SG	24 hours	S	Yes	I		X		X	
31	Safety Injection Accumulator Isolation Valve Position	Closed/not closed	1 / valve	24 hours	S	Yes	I				X	
32	Safety Injection System Suction Strainer Differential Pressure	0 to 5 psid	1 / train	1 year	S	Yes	I				X	
33	Source Range Neutron Flux	0.05 to 5 x 10^4 n/cm^2-s	2	1 year	S	Yes	I		X			

Table 7.5-1—Inventory of Post-Accident Monitoring Variables
Sheet 4 of 4

No	Variable	Range	Minimum Channels Required	Duration	Safety Class	EQ[1] per IEEE Std 323-1974	Seismic Qualification	Type				
								A	B	C	D	E
34	Subcooling Margin	611°F Subcooling Margin to 2088°F Superheat	2	24 hours	S	Yes	I	X	X			
35	Vent Stack Aerosol Activity	See Table 11.5-1, R-4, R-5	1	1 year	NS	No	NSC					X
36	Vent Stack Iodine Activity	See Table 11.5-1, R-4, R-5	1	1 year	NS	No	NSC					X
37	Vent Stack Gas Activity	See Table 11.5-1, R-4	1	1 year	NS	No	NSC					X
		See Table 11.5-1, R-6	1	1 year	NS-AQ	Yes	II					X

Notes:

1. Environmental Qualification.

Next File