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 are 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 accident monitoring variables based on 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 addition 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 some limited backup annunciation functions if the PICS is unavailable.

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

7.5.1.2 Accident Monitoring Instrumentation

The accident monitoring instrumentation (AMI) provides plant process variable information and system status, known as post accident monitoring (PAM) variables, 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 AMI utilizes the components of existing safety-related and non-safety-related I&C systems to accomplish AMI functions. The primary operator interface in the MCR for displaying all PAM variables is the non-safety-related PICS. If the PICS is not available, the safety-related SICS is used. The protection system (PS), safety automation system (SAS), process automation system (PAS), 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 Facilities

The description of the emergency response facilities (ERF) in this section is limited to the system interface with the plant I&C systems. The ERF consists of the safety parameter display system (SPDS), Emergency Response Data System (ERDS), and technical support center (TSC). These systems and facilities 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 via a firewall to systems external to the plant I&C systems. Details of the architecture of PICS is 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 primary SPDS display and the SICS provides a backup SPDS display.

7.5.1.4 Bypass and Inoperable Status Indication

Bypassed and inoperable status indication (BISI) of safety related system 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 systems 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 requirements listed in NUREG-0800 (Reference 10), Section 7.5, apply to the I&C systems listed in Section 7.5.1.

Compliance to 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”.
- 10 CFR 52.47 (b)(1), “ITAAC for Standard Design Certification”.

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

The following are TMI related requirements that apply to the AMI described in Section 7.5.1.

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

If any PAM Type A, B, and C 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

Emergency feedwater (EFW) flow to each steam generator (SG) is provided in the MCR. Details on the EFW flow sensors are described in Section 10.4.9.

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 intensity (high level) monitors are provided by the radiation monitoring system (RMS) described in Section 11.5.
- Noble gas effluent monitoring at all potential accident release points are provided by the RMS described in Section 11.5.

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

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

- The reactor vessel water level indication is provided by the reactor pressure vessel water level measurement system described in Section 7.1.
- 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.

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

The post accident monitoring 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 PICS and is backed by 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 variables, including post accident monitoring variables and system variables over their anticipated ranges for normal operation, for AOO, and for 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 with Regulatory Guide 1.97 and BTP 7-10

The guidance of RG 1.97, Revision 4, will be used to select the accident monitoring variables during detailed design. With clarifying regulatory positions, RG 1.97, Revision 4, endorses 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). The development of these guidelines and procedures is discussed in Section 13.5. When these procedures are complete and verified, they will be used to develop a complete accident monitoring instrumentation list.

Minimum Inventory of Accident Monitoring Variables

The minimum inventory list of accident monitoring variables is provided in Table 7.5-1—Minimum Inventory of Post Accident Monitoring Variables. This minimum inventory list was developed by examining those features of the EPR design that must be used to implement the EOP methodology.

Methodology for Selecting Final List of Accident Monitoring Variables

To meet the guidance of RG 1.97 and Reference 1, a systematic step-by-step review of the plant specific EOPs for the U.S. EPR is required. See Section 18.8 and Section 13.5 for more information on U.S. EPR procedure development.

The complete accident monitoring instrumentation list will be documented in a table format that includes the following:

- Variable name that indicates the variable function.
- Variable Type (A, B, C, D or E).
- Range.
- Safety classification (1E or non-1E).
- Environmental and Seismic Qualification.
- Minimum number of instruments required.
- Monitoring duration for the variable.
- Reason for the parameter and any parameter comments.

Performance Assessment

A performance assessment of each of the following performance criteria specified in Reference 1 will be conducted and the results documented:

- Range.
- Accuracy.
- Response time.
- Required instrument duration.
- Reliability.

In conformance with Reference 1, a graded approach will be used to develop setpoints associated with accident monitoring variables based on their importance to safety.

Criteria for Selection of Variable Types

In accordance with RG 1.97, Revision 4, and Reference 1, the accident monitoring variables are selected and the variable types are determined according to its accident management function. These variables are the primary source of 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 will include those variables that are associated with contingency actions that are within the plant licensing basis and may be identified in written procedures.

Type A variables are a subset of those necessary to implement the plant specific EPGs or the plant specific EOPs.

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 as defined in Reference 1.

Critical safety functions are those safety functions that are essential to prevent a direct and immediate threat to the health and safety of the public. These accomplish or maintain:

- Reactivity control.
- Reactor core cooling.
- The RCS integrity.
- Primary reactor containment integrity.
- Radioactive effluent control.

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.

Accident Monitoring Instrumentation Criteria

The I&C systems that perform the AMI functions are designed in accordance with the performance (criterion 5), design (criterion 6), qualification (criterion 7), and display criteria (criterion 8) of Reference 1 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 supervisory control system level (level 2) consists of data processing related to HMI for process control and monitoring. The SICS and PICS are the systems which make up the supervisory control system level and are implemented using digital computer platforms.

The software and hardware development of the SICS is performed in accordance with the quality criterion for digital computers specified in IEEE 7-4.3.2-2003 (Reference 2).

To minimize the potential for non-safety digital control system failures that could challenge safety systems, non-safety digital control system hardware and software is developed using a structured process similar to that applied to safety system software; however, the process is tailored to account for the lower safety significance. The hardware and software development process of PICS is described in Section 7.7.

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 system has been bypassed or deliberately rendered in-operative continued indication of the bypassed condition for each affected safety group 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 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

Diversity is provided for the processing and display of indications and alarms necessary to alert the operator to abnormal plant conditions, including Type A, B, and C accident monitoring variables as defined in RG 1.97, Revision 4. These accident monitoring variables are acquired and processed by the safety classified PS and SAS, then transmitted to the safety classified SICS for display.

Also, the non-safety classified PAS provides diverse processing of sensor information because the PAS obtains sensor information independently of the PS and SAS software. Type A, B, and C accident monitoring variables are acquired by the PAS from the PS or SAS via isolation devices, processed by PAS, and then transmitted to the non-safety classified PICS for display. Therefore, the PAS and the PICS provide a redundant and diverse path for display of the variables.

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 and non-safety I&C systems. Compliance to 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. Requirements of Reference 3 for safety systems meet or exceed the requirements of the endorsed version, IEEE Std 603-1991. A comparison of IEEE Std 603-1991 and IEEE 603-1998 is described in Digital Protection System Topical Report ANP-10281P (Reference 9).

7.5.2.2.8 Self Test Provisions

Branch Technical Position BTP 7-17 (Reference 8), provides guidance on the use of self-testing features of digital I&C system. The SICS is designed to maximize the use of automated self-testing features to minimize the burden on plant personnel. The safety-related qualified display system (QDS) within the SICS has the capability to perform automatic self-testing to verify its ability to perform the intended functions. This self-testing feature includes, but is not limited to, the availability of components such as processors, communication and link modules, power supplies, and input-output modules. The positive aspect of these self-testing features is to provide a mechanism for detecting all detectable failures. Furthermore, the positive aspects of the self-test features are not compromised by the additional complexity added to the

system design. The self-test features of the SICS do not affect the ability of the system to perform its safety functions.

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. IEEE 7-4.3.2-2003, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations," Institute of Electrical and Electronics Engineers, 2003.

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. NUREG-0800, BTP 7-17, "Guidance on Self Test and Surveillance Provisions," Nuclear Regulatory Commission, March 2007.

9. ANP-10281P, Revision 0, "U.S. EPR Digital Protection System Topical Report," AREVA NP Inc., March 2007.

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

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

Variable Description
Power Range Nuclear Flux
Intermediate Range Nuclear Flux
Source Range Nuclear Flux
Control Rod Drive Mechanism (CRDM) Position
Generator output and exciter breaker position indication
24 Vdc I&C power
Emergency Power Supply System 6.9 kV Bus Voltage
PZR level
PZR steam temperature
PZR pressure
PZR heater status (emergency supplied)
PZR auxiliary spray valve indication
PZR normal spray valve indications
PSRV position indication
RCS hot leg temperature wide range (WR)
RCS hot leg temperature narrow range (NR)
RCS cold leg temperature (WR)
RCS cold leg temperature (NR)
RCS hot leg pressure (WR)
RCS hot leg pressure (NR)
Incore Thermocouple Temperature
Medium Head Safety Injection (MHSI) flow
Low Head Safety Injection (LHSI) flow
LHSI cooler inlet temperature (IRWST temperature)
IRWST level
Safety Injection Accumulator (SIA) Level (WR)
SIA isolation valve position
LHSI hot leg injection flow
Component Cooling Water System (CCWS) flow
CCWS temperatures
Essential Service Water System (ESWS) flow
ESWS temperatures
Containment temperature

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

Variable Description
Containment pressure
Pressurizer relief tank (PRT) pressure
PRT temperature
PRT level
RCS loop flow
RCS boron concentration
Extra Borating System (EBS) flow
CVCS charging flow
CVCS letdown flow
Volume Control Tank (VCT) level
Reactor pressure vessel high point vent valve position indication
Containment hydrogen monitors
RCP motor amps
Reactor vessel level indication
Steam Generator (SG) level (WR)
SG Level (NR)
SG pressure
Main steam flow
SG blowdown flow
Emergency feedwater (EFW) flow
Main feedwater flow (MFW)
Startup shutdown system (SSS) flow
Condensate flow
Main steam isolation valve (MSIV) position indication
Main steam safety valve (MSSV) position indication
Main steam relief isolation valve (MSRIV) position indication
Condenser vacuum
Containment isolation valve position indication (not including check valves)
Main steam line radiation monitors
Turbine Building main condenser beta activity monitor
SG secondary side sample radiation monitors
SG blowdown radiation monitors
Containment high range radiation monitors