Westinghouse Non-Proprietary Class 3

WCAP-16097-NP-A
Appendix 1, Revision 0
(Previously released as CENPD-396-NP, Appendix 1)

May 2003

Common Qualified Platform Post Accident Monitoring Systems

Common Qualified Platform
Post Accident Monitoring Systems

WCAP-16097-NP-A
Appendix 1, Revision 0

CENPD-396-NP-A
Appendix 1, Revision 2

May 2003

Revision Abstract

Revision 00:
This is the original issue of this document. This document was previously released as CENPD-396-NP, Appendix 1. It is being prepared to create the accepted version in accordance with the USNRC Safety Evaluation dated February 24, 2003. The previously released document CENPD-396-NP, Appendix 1, Revision 1 has been modified as follows:

- A document titled, "Changes to the Westinghouse Common Qualified Platform Post Accident Monitoring Systems, CENPD-396-P, Appendix 1, Revision 1" was provided to the NRC via LTR-NRC-02-41, dated August 14, 2002. The changes identified in that document have been incorporated into this revision.
- Minor changes were made to clarify some of the technical descriptions.
- Correction of typographical errors.
- Minor document format changes were made.
- The Reference to the Software Program Manual for Common Q Systems has been updated.
- Reference to the CENP Quality Assurance Procedures Manual was replaced with the Westinghouse Quality Management System and its implementing procedures.

Table of Contents

A1.0 Purpose and Scope

The purpose of this Post Accident Monitoring System (PAMS) appendix is to provide the functional requirements and the conceptual design description of the PAMS.

The scope of the PAMS appendix is to provide the functional requirements and the conceptual design of the system based on Common Q components. The requirements include PAMS functional design, testing, major Man Machine Interface functions, system block diagrams, and the interface with the Plant Monitoring Computer / plant Safety Parameter Display System. The system hardware and software descriptions, the complete system interface requirements and the failure modes and effects analysis are also included.

Each PAMS system is comprised of two redundant and isolated channels. Instruments needed to produce the signals used by the PAMS are not included in the PAMS requirements.

The PAMS includes one or more of the following subsystems:

- Inadequate Core Cooling Monitoring System (ICCMS) / Subcooled Margin Monitor (SMM) / Core Exit Thermocouple Monitoring System (CETMS)
- Heated Junction Thermocouple (HJTC) System / Reactor Vessel Level Monitoring System (RVLMS)
- Qualified Safety Parameter Display System (QSPDS) / typically includes all of the above

Brackets in this document indicate proprietary information. The bracket denoting the end of a proprietary segment of this report may appear one or more pages following the bracket denoting the start of the proprietary segment. As a result, care should be exercised in determining what information in this report is proprietary.

A1.1 PAMS Functional Requirements

A1.1.1 PAMS Overview

A specific PAMS implementation includes one or more of the following subsystems:

- Heated Junction Thermocouple (HJTC) System / Reactor Vessel Level Monitoring System (RVLMS)
- Subcooled Margin Monitor (SMM)

- Core Exit Thermocouple Monitoring System (CETMS)
- Inadequate Core Cooling Monitoring System (ICCMS), which includes an SMM, a CETMS, and an HJTC System (HJTCS)
- Qualified Safety Parameter Display System (QSPDS), which includes all of the above systems.

The PAMS is a Class 1E safety related alarm and display system. Each PAMS system consists of two independent channels of equipment (Channels A & B) which acquire and process two channels of inputs. The two channels of equipment are located in one or more cabinets, depending upon the plant. The channels are physically separated and electrically isolated from each other. The details of the PAMS signal transducers are discussed in this appendix only to the extent necessary to understand the use of their outputs, which are used as inputs to the PAMS data acquisition equipment.

Depending upon the implementation, the PAMS system channel inputs may include plant process signals, core exit thermocouples (CETs) and heated junction thermocouples (HJTCs).

Depending upon the implementation, each PAMS system channel may provide HJTCS heater power outputs, and provides analog output values for display on meters / recorders, contact outputs for use by the plant annunciator system, isolated data link data for display on an Operator's Module (OM), and isolated data link data for use by the Plant Monitoring Computer (PMC) or the primary Safety Parameter Display System (SPDS).

Each channel of the SMM monitors pressurizer pressure, hot and cold leg temperatures to detect and alarm subcooling margin.

Each channel of the CETMS monitors core exit thermocouple temperatures to detect and alarm inadequate core cooling conditions.

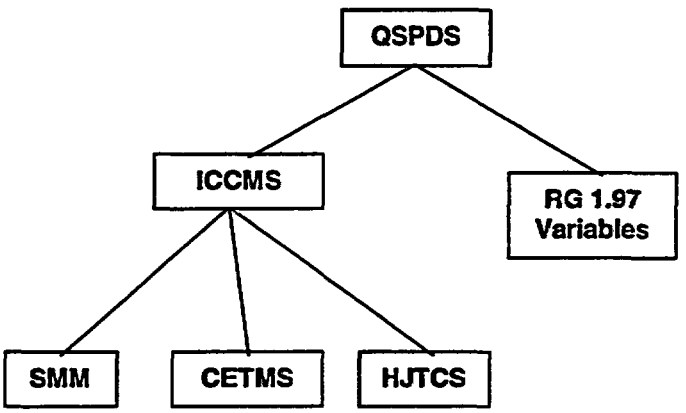
Each channel of the HJTCS/ RVLMS monitors 8 heated / unheated thermocouple pairs to provide the reactor vessel collapsed liquid level above the core. When a split HJTC probe is used, a separate level measurement is provided for the Upper Head and for the Plenum.

Each channel of the ICCMS monitors CET temperatures, pressurizer pressure, hot and cold leg temperatures, and 3 unheated thermocouple temperatures in the reactor head, to detect and alarm Inadequate Core Cooling (ICC) conditions. Saturation margins are calculated for the Reactor Coolant System (RCS) hot and cold leg temperatures, the reactor

vessel head (using the top 3 unheated thermocouples), and at the core exit.

Each channel of the QSPDS provides the combined functions of the ICCMS (i.e., SMM, CETMS and HJTCS/ RVLMS systems). Additional Regulatory Guide 1.97 safety related parameters are also monitored, alarmed and displayed as a backup to the plant Safety Parameter Display System (SPDS).

The relationship of these individual PAMS systems is shown in the following figure:



Since the QSPDS functions encompass the ICCMS / SMM / CETMS and the HJTCS/ RVLMS functions, the PAMS functional requirements and descriptions provided herein are based upon those for the generic CE Nuclear Power (CENP) QSPDS, Reference A1.8.1.

Plant specific PAMS designs can be developed from those defined in this appendix.

The PAMS block diagram is provided in Figure A1.1.1-1. The PAMS design is based on the AC160 system components and the S600 I/O equipment, collectively referred to as the Common Q building blocks, discussed in the body of this topical report. Each aspect of the block diagram is discussed in the following sections. Section A1.3.1.1 provides a summary of the components and their use, as shown in the Figure.

Figure A1.1.1-1
PAMS Block Diagram

[ ]

A1.1.1.1 PAMS Maintenance and Test Panel Functions

Each PAMS channel communicates with a Maintenance and Test Panel (MTP) located in the PAMS channel cabinet. The MTP is comprised of a flat panel display system, as discussed in the body of this topical report.
[ ]

A1.1.1.2 PAMS Inputs

The generic PAMS inputs include the inputs required to support the Inadequate Core Cooling detection function (i.e., the combined CETMS / HJTCS/ ICCMS / SMM functions) and typical inputs as required to support the backup Safety Parameter Display System (SPDS) function (see discussion below). It is expected that the number and type of specific SPDS inputs may vary from plant to plant.

The PAMS system uses two sets of inputs, one per channel, for all input parameters. A list of input types is provided below. Some spare inputs are also included in the count.

In addition, each PAMS channel monitors its cabinet temperature and actuates a digital output if the temperature is greater than or equal to a predefined setpoint. At least 2 inputs shall be used for monitoring this temperature.

All the digital inputs described below apply only for a PAMS which includes QSPDS functions. Many of the analog inputs described are not needed for the ICC condition monitoring. All the analog inputs shown in Table A1.1.2.3.1-2 are used by the ICC condition monitoring function of PAMS, and are the minimum number of inputs for the ICC monitoring function.

The PAMS inputs can be summarized as follows:
[ ]

The PAMS inputs may be further described as follows:
[ ]

A1.1.1.3 PAMS Outputs

The two PAMS channels process the channel inputs so as to provide ICC condition monitoring, including reactor vessel level monitoring, and provide the following outputs:

- contact digital outputs

- analog outputs
- data link communications to/from the MTP and to/from the PAMS Operators' Module (OM)
- The MTP, discussed in Section A1.1.1.1, provides a data link interface to the plant Safety Parameter Display System (SPDS).

The OM and the MTP are discussed below, in Section A1.1.1.6, PAMS Human Machine Interface.

A1.1.1.4 PAMS Bypasses

[ ]

A1.1.1.5 PAMS Failure Modes

The PAMS shall be designed for operation under component failure or loss of electrical power as defined in the Failure Modes and Effects Analysis (FMEA) in Section A1.6.

Since the proposed PAMS channel implementation includes extensive hardware and software diagnostic capability, as well as redundant channel design features, the channel is fault tolerant to a great extent. Fault tolerance is discussed in Section A1.3.

A1.1.1.6 PAMS Human Machine Interface

The PAMS Human Machine Interface (HMI) is provided by the OM and the MTP. Additional PAMS operator interfaces are described in Section A1.1.2.2.7, Program Interfaces. The HMI shall be designed per accepted Human Factors Engineering (HFE) principles. Both the MTP and OM shall include display and diagnostic capabilities unavailable in the present design. HMI provisions are described in sections A1.1.2.3 (OM) and A1.1.2.4 (MTP).

A1.1.1.7 PAMS Functional Diversity

[ ]

A1.1.2 PAMS Functional Requirements Detail

This document is a generic document describing the functional and design requirements for a PAMS . The functional requirements defined herein include all the functions presently implemented in CENP's QSPDS.

The PAMS described in this appendix includes the Inadequate Core Cooling (ICC) detection function and the Reactor Vessel Level Monitoring System (RVLMS) function. This section describes how the ICC and RVLMS functions in the PAMS are used to detect ICC conditions along with other instruments.

Additional PAMS input variables are based on the QSPDS design, which serves as a backup SPDS.

The scope of information in this section includes:

1. The design bases for the PAMS ;

2. A compilation of functional and design requirements and criteria for the PAMS based on the functional design specification, Reference A1.8.1.

3. Documentation of the CENP approach to meeting the design bases of Section A1.1.2.1 in this document, and in Section 5 of Reference A1.8.1.

4. Specification of the functions, inputs, application software algorithms, and display requirements for the design bases of Section A1.1.2.1.

A description of the PAMS display design requirements is included in Sections A1.1.2.2.10.4, A1.1.2.3.1, and A1.1.2.4.1.

For a specific plant PAMS upgrade, additional documents are required in conjunction with this document as described in the SPM, Reference A1.8.9.

[ ]

A1.1.2.1 PAMS Design Bases

The PAMS design bases are the same as those in Reference A1.8.1 for CENP's QSPDS, and are as follows:

[ ]

A1.1.2.1.1 PAMS Design Basis Events

[ ]

A1.1.2.1.2 PAMS Timing

The PAMS channels shall have a response time consistent with that of the present QSPDS implementation, as defined in Section A1.1.2.2.5, Programming Timing and Input Sample Rates.

A1.1.2.2 PAMS System Requirements

The PAMS system requirements are defined in the following sections.

A1.1.2.2.1 PAMS Overall System Design Requirements

The following subsections define how the overall design requirements for the QSPDS, discussed in Reference A1.8.1, apply to the PAMS.

A1.1.2.2.1.1 Single Failure Requirement

[ ]

A1.1.2.2.1.2 Separation Requirements

[ ]

A1.1.2.2.1.3 Power Source Requirement

[ ]

A1.1.2.2.1.4 Availability Requirements

[ ]

A1.1.2.2.1.5 Quality Assurance

The quality assurance of the PAMS shall utilize the Westinghouse Quality Management System and its implementing procedures as augmented by the Common Q Software Programming Manual, Reference A1.8.9.

A1.1.2.2.1.6 Indication Requirement

[ ]

A1.1.2.2.1.7 PAMS Display Location

The PAMS display device shall be capable of control panel mounting (surface cutouts), similar to present QSPDS displays.

A1.1.2.2.1.8 PAMS Isolation

[ ]

A1.1.2.2.1.9 Testing, Calibration and Maintenance Requirements

[ ]

A1.1.2.2.1.10 Environmental and Seismic Qualification

[ ]

A1.1.2.2.1.11 Operability Requirements

The PAMS shall be capable of operation during the following plant operating modes:

- Power operation
- Hot standby
- Hot Shutdown
- Start-up
- Cold Shutdown

PAMS operation during normal and abnormal conditions is discussed in Section A1.1.2.2.1.4.

A1.1.2.2.1.12 Alarm and Annunciation Requirements

[ ]

A1.1.2.2.1.13 Accuracy Requirements

[ ]

A1.1.2.2.1.14 Timing Requirement

[ ]

A1.1.2.2.1.15 Testing Requirements

[ ]

A1.1.2.2.1.16 Codes and Standards

[ ]

A1.1.2.2.2 PAMS Inputs

[ ]

The accuracies for the PAMS inputs are defined in Section A1.1.2.2.6.

A1.1.2.2.3 PAMS Outputs

[ ]

A1.1.2.2.4 PAMS Program Structure

The PAMS software development, testing, verification and validation will be in accordance with the Software Program Manual for Common Q Systems, Reference A1.8.9.

[ ]

A1.1.2.2.10.4 PAMS Displays

PAMS displays are provided on the OM and the MTP. The OM and MTP are described in Sections A1.1.2.3 and A1.1.2.4, below.

A1.1.2.3 Operator Interface / Operator's Module

[ ]

The OM shall be capable of being located in the control room. It is comprised of the same flat panel display system hardware as the MTP. The OM shall be mounted to facilitate operator input via its touch screen if possible. If use of the touch screen is not practical, operator entry shall be via a Page Control Module (PCM). Operator entries by either the touch screen or the PCM shall have the same effect.

[ ]

Additional information on the OM is provided in Section A1.3.2

A1.1.2.3.1 Operator's Module Displays

[ ]

See Section A1.1.2.4.1 for a discussion of OM indications when the Bypass permissive is actuated and when it is un-actuated.

A1.1.2.3.2 Operator Inputs to the Operator's Module

[ ]

A1.1.2.4 Maintenance and Test Panel Interface

The MTP shall be located in the PAMS channel cabinet. It is comprised of the same flat panel display hardware as the OM. The MTP shall be mounted in the cabinet so that use of the optional PCM is not required.

[ ]

Additional information on the MTP is provided in Section A1.3.3

A1.1.2.4.1 MTP Displays

[ ]

A1.1.2.4.2 Operator / Technician Inputs to the MTP

[ ]

Detailed design requirements for the Bypass and test initiation input displays will be specified during the PAMS design phase.

A1.2 System Description

A1.2.1 Overview

[ ]

A1.2.1.1 PAMS Processor Overview

[ ]

A1.2.1.2 PAMS OM Overview

[ ]

A1.2.1.3 MTP Overview

[ ]

A1.2.1.4 PAMS Watchdog Timer

[ ]

A1.2.2 PAMS Design Implementation

[ ]

A1.3 Hardware Description

[ ]

A1.4 Software Description

[ ]

A1.5 System Interfaces

[ ]

A1.6 Failure Modes and Effects Analysis (FMEA)

[ ]

A1.7 10 CFR 50.59 Evaluation

This evaluation addresses the generic issues associated with the replacement of the existing Post Accident Monitoring System (PAMS) with a system based upon the Common-Qualified Platform, as delineated in this appendix.

[ ]

The PAMS is a Class 1E safety related alarm and display system.

[ ]

This evaluation is required because of the replacement of the existing post accident monitoring system with a Common-Qualified Platform-based system. Post Accident Monitoring capability is required by NUREG 0737, is reflected in plant Technical Specifications, and is described in the plant Final Safety Analysis Report (FSAR).

A1.7.1 Safety Evaluation Summary

[ ]

A1.7.2 Unreviewed Safety Question Determination

A1.7.2.1 Malfunctions

[ ]

A1.7.2.1.1 Effects on the Probability of Occurrence of Previously Evaluated Malfunction of Equipment Important to Safety

[ ]

A.1.7.2.1.2 Effects on the Consequences of a Previously Evaluated Malfunction of Equipment Important to Safety

[ ]

A.1.7.2.1.3 Possibility of a Malfunction of a Different Type than Previously Evaluated

[ ]

A.1.7.2.2 Accidents

[ ]

A.1.7.2.2.1 Effect on the Probability of Occurrence of Previously Evaluated Accidents

[ ]

A.1.7.2.2.2 Effects on the Consequences of Previously Evaluated Accidents

[ ]

A1.7.2.2.3 Possibility of an Accident of a Different Type than Previously Evaluated

[ ]

A.1.7.2.3 Impact on the Margin of Safety

[ ]

A.1.7.3 Safety Determination

[ ]

A1.8 References

The following is a list of references, codes, standards, and guidelines upon which the PAMS design is based. These documents are applied as referred to in this appendix.

CENP Documents

A1.8.1 Functional Design Specification for a Qualified Safety Parameter Display System, NPROD-ICE-3201, Rev. 02, 11/30/82.

A1.8.2. Functional Design Description for the Qualified Safety Parameter Display System for San Onofre Nuclear Generating Station Unit 2, 1370-ICE-3218, Rev. 02, 12/14/83.

A1.8.3 Functional Design Specification for the Reactor Vessel Level Monitoring System, NPROD-ICE-3200, Rev. 02.

A1.8.4 Functional Design Description for the Qualified Safety Parameter Display System Displays for San Onofre Nuclear Generating Station Unit 2, 1370-ICE-3220, Rev. 01.

A1.8.5 AC110 2.3 System Software Functional Description #BDS 005 438

A1.8.6 Functional Design Description for the Reactor Vessel Level Monitoring System, NPROD-ICE-3200, Rev. 03.

A1.8.7 Class 1E Qualification, Qualification of Class 1E Electrical Equipment, CENPD-255A, Revision 3, 10/85

A1.8.8 Qualification of C-E Instrumentation Equipment, CENPD-182

A1.8.9 Software Program Manual for Common Q Systems, CE-CES-195-NP-A, Revision 2

Codes and Standards

A1.8.10 10 CFR 50 Licensing and Utilization of Production Facilities, Appendix A, General Design Criteria (GDC)

1. GDC 1, Quality Standards and Records
2. GDC 2, Design Bases for Protection Against Natural Phenomenon
3. GDC 3, Fire Protection
4. GDC 4, Environmental and Missile Design Bases
5. GDC 13, Instrumentation and Control

6. GDC 18, Inspection and Testing of Electric Power Systems
7. GDC 24, Separation of Protection and Control Systems

A1.8.11 10 CFR 50, Appendix B, Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Facilities

A1.8.12 Regulatory Guide 1.75, Physical Independence of Electric Systems, Revision 2, 9/78

A1.8.13 Regulatory Guide 1.89, Qualification of Class 1E Equipment for Nuclear Power Plants, Revision 1, 6/84

A1.8.14 Regulatory Guide 1.97, Instrumentation for Light Water Cooled Nuclear Power Plants to Assess Plant Conditions During and Following an Accident, Revision 3, 5/83

A1.8.15 Regulatory Guide 1.100, Seismic Qualification of Electric Equipment for Nuclear Power Plants, Revision 2, 6/88

A1.8.16 Regulatory Guide 1.118, Periodic Testing of Electric Power and Protection Systems, Revision 2, 6/78

A1.8.17 Regulatory Guide 1.152, Criteria for Programmable Digital Computers in Safety Systems of Nuclear Power Plants, Revision 1, 11/96

A1.8.18 Regulatory Guide 1.153, Criteria for Safety Systems, 1996

A1.8.19 Regulatory Guide 1.168, Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants, 1997

A1.8.20 Regulatory Guide 1.169, Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants, 1997

A1.8.21 Regulatory Guide 1.171, Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants

A1.8.22 Regulatory Guide 1.172, Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants, 1997

A1.8.23 Regulatory Guide 1.173, Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants, 1997

A1.8.24 NUREG-0588, Interim Staff Position on Environmental Qualification of Safety Related Electrical Equipment, Revision 1, 7/81

A1.8.25 NUREG-0696, Guidelines for Emergency Response Facilities, Revision

A1.8.26 NUREG-0700, Guidelines for Control Room Design Reviews

A1.8.27 NUREG-0737, Clarification of TMI Action Plan Requirements, 1980

A1.8.28 NUREG-0814, Methodology for Evaluation of Emergency Response Facilities

A1.8.29 NUREG-0835, Human Factors Acceptance Criteria for the Safety Parameter Display System

A1.8.30 NUREG/CR-6421, A Proposed Acceptance Process for Commercial Off the Shelf (COTS) Software in Reactor Applications, 1996

A1.8.31 IEEE 279-1971, Criteria for Protection Systems for Nuclear Power Generating Stations

A1.8.32 IEEE 603-1991, Standard Criteria for Safety Systems for Nuclear Power Generating Stations

A1.8.33 IEEE 308-1974, Standard Criteria for Class 1E Electric Systems for Nuclear Power Generating Stations

A1.8.34 IEEE 323-1983, Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations

A1.8.35 IEEE 338-1987, Standard Criteria for the Periodic Surveillance Testing of Nuclear Power Generating Station Safety Systems

A1.8.36 IEEE 344-1987, Recommended Practice for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations

A1.8.37 IEEE 384-1992, Standard Criteria for Independence of Class 1E Equipment and Circuits

A1.8.38 IEEE 7-4.3.2-1993, Standard Criteria for Programmable Digital Computer Systems in Safety Systems of Nuclear Power Generating Stations

A1.8.39 ANSI/ANS 4.5-1980, Criteria for Accident Monitoring Functions in Light Water Cooled Reactors

A1.8.40 ANSI/ANS 4.6-Draft, Functional Criteria for On-Line Monitoring – Transient Reconstruction in Light Water Reactors

A1.8.41 ANSI/ANS MC96.1-1975, Temperature Measurement Thermocouples

A1.8.42 ASME Steam Tables, Thermodynamic and Transport Properties of Steam, Sixth Edition

A1.8.43 ISA-S67-04, Setpoints for Nuclear Safety Related Instrumentation Used in Nuclear Power Plants, 1994

A1.8.44 ANSI C37.90.1, Standard Surge Withstand Capability (SWC) Tests for Protective Relays and Relay Systems, 1989

A1.8.45 EPRI NP-5652, Guideline for Utilization of Commercial Grade Items in Nuclear Safety Related Applications

A1.8.46 EPRI Topical Report TR-102323, Guidelines for Electromagnetic Interference Testing in Power Plants, 1997

A1.8.47 EPRI Topical Report TR-106439, Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications, 1996

A1.8.48 MIL-STD-461D, Military Standard Electromagnetic Interference Characteristics Requirements for Equipment, 1993

A1.8.49 MIL-STD-462D, Military Standard Electromagnetic Interference Characteristics, Measurement of, 1993

A1.8.50 EPRI TR-107330, Generic Requirements Specification for Qualifying a Commercially Available PLC for Safety Related Applications in Nuclear Power Plants