Westinghouse Non-Proprietary Class 3

WCAP-16592-NP
Revision 0

June 2006

Software Hazard Analysis of AP1000 Protection and Safety Monitoring System

WCAP-16592-NP
Revision 0

Software Hazard Analysis of AP1000 Protection and Safety Monitoring System

Raymond R. Senechal
Principal Engineer, Reactor Protection Systems II

June 2006

Reviewer: Joseph E. Burns*
Principal Engineer, Reactor Protection Systems II

Approved: Timothy C. Wilson*, Project Manager
Protection and Monitoring Systems

Approved: Larry E. Erin*, Manager
Reactor Protection Systems I

*Electronically approved records are authenticated in the electronic document management system.

Westinghouse Electric Company LLC
P.O. Box 355
Pittsburgh, PA 15230-0355

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ACRONYMS AND TRADEMARKS

AC160	Advant Controller Series 160
AF100	Advant Fieldbus 100
AOV	Air Operated Valve
BCC	Bistable/Coincidence Logic Cabinet
BPL	Bistable Processor and Logic
CIM	Component Interface Module
CMF	Common Mode Failure
COL	Combined Operating License
CRC	Cyclic Redundancy Check
CS	Communication Section (AC160 PM646A Module)
DAS	Diverse Actuation System
DCD	Design Control Document
DDS	Data Display and Processing System
DIV	Division
DO	Digital Output
DSP	Dedicated Safety Panel
ESF	Engineered Safety Feature
ESFAS	Engineered Safety Feature Actuation System
FMEA	Failure Modes and Effects Analysis
FPD	Flat Panel Display
HOV	Hydraulic Operated Valve
HSI	Human System Interface
HSL	High Speed Link
ICP	Interface Communication Processor
ILC	Interposing Logic Cabinet
ITP	Interface and Test Processor
I/O	Input/output module
LCL	Local Coincidence Logic
mA	Milliamps
MCR	Main Control Room
MOV	Motor Operated Valve
MTP	Maintenance and Test Processor
NIC	Nuclear Instrumentation Cabinet
NIMOD	Nuclear Instrumentation Module
NIS	Nuclear Instrumentation Subsystem
PC	Personal Computer
PLC	Programmable Logic Controller
PLS	Plant Control System
PM	Processor Module (AC160 PM646A Module)
PMS	Protection and Safety Monitoring System
PR	Power Range
PS	Processor Section (AC160 PM646A Module)
QDPS	Qualified Data Processing System
RPS	Reactor Protection System

LIST OF ACRONYMS AND TRADEMARKS (cont.)

RSR	Remote Shutdown Room
RT	Reactor Trip
RTD	Resistance Temperature Detector
RTDN	Real Time Data Network
SHA	Software Hazard Analysis
SOV	Solenoid Operated Valve
WDT	Watchdog Timer
WEC	Westinghouse Electric Company LLC

Advant, AC160 and AF100 are trademarks of ABB Automation Systems GmbH.

All other product and corporate names used in this document may be trademarks or registered trademarks of other companies, and are used only for explanation and to the owners' benefit, without intent to infringe.

REFERENCES

Following is a list of references used throughout this document.

1. WCAP-16438-P, Rev. 1, "FMEA of AP1000 Protection and Safety Monitoring System" (Proprietary)

2. APP-GW-GL-700, "AP1000 Design Control Document"

3. WCAP-16096-NP-A, Rev. 1A, "Software Program Manual for Common Q Systems"

1 INTRODUCTION

1.1 PURPOSE

The purpose of this report is to present the Software Hazard Analysis (SHA) for the AP1000 Protection and Safety Monitoring System (PMS). This document compliments the Failure Mode and Effects Analysis (FMEA) (Reference 1) and will satisfy the Combined Operating License (COL) item identified in the Design Control Document (DCD) (Reference 2) Paragraph 7.2.3.

1.2 SCOPE

This report is based on the detail design of the PMS (Figure 2-2), the analysis of the FMEA (Reference 1) and the software design, implementation, validation and verification activities performed in accordance with the Software Program Manual (SPM) (Reference 3). This analysis is restricted to the safety inputs, components located in the PMS cabinets, and the communication between redundant divisions. The analysis does not include the components involved in process sensing, the actuated devices, initiation circuitry or the devices for manual actuation of the Reactor Protection System (RPS) trip and/or Engineered Safety Feature Actuation System (ESFAS) functions. The emphasis is on the Programmable Logic Controller (PLC) software to demonstrate that potential software hazards have been identified and compensating design features are being addressed.

1.3 CONCLUSIONS

The analysis performed reflects a current status of the PMS. For this reason, the Software Hazard Analysis (SHA) may be revisited during the software life cycle for potential or new hazards. The SHA confirmed that with adequate document review, code inspection and software testing, the PMS software can perform the safety functions as designed. The application software in the redundant divisions is functionally similar. Common mode failure of the PMS software is accommodated by the Diverse Actuation System (DAS).

As identified in the Safety Hazard Control Verification Method Column (Table 5-1), the correct operation of the software is dependent on the software code review, change in software requirements, inspection, verification and validation. The program code and system interfaces for events, faults, and conditions that could cause or contribute to undesired events affecting safety are analyzed and documented as soon as a software coding phase is complete. Testing requirements and test case requirements are developed for incorporation into the corresponding test documents. These tasks are contained in the SPM (Reference 3). In addition, the software safety plan (Reference 3) defines the software safety-related activities that are carried out in response to changes made in specifications, requirements, design, code, equipment, test plans, and environment and user documentation.

The analysis demonstrates that the PMS software provides a low probability of creating hazards even when it fails. It also shows that a single failure in the plant does not create software hazards. The PMS design is capable of performing its protective functions with high reliability.

2 ARCHITECTURE OVERVIEW

The overall architecture of the PMS is shown, in simplified form, in Figure 2-1. This diagram shows the communication interfaces between the various cabinets and process stations that make up the safety system that consists of four divisions. Divisions B and C are identical in content and contain a full complement of equipment. Divisions A and D each contain a subset of the equipment (no Qualified Data Processing System (QDPS)) to provide a four channel redundancy where specified by the system requirements.

This analysis focuses on Division B as being representative of each division. When differences between the divisions are significant to the analysis, it is so noted. Figure 2-2 provides a more detailed diagram of the division's equipment and is representative of the other divisions. The analysis considers each process station or subsystem as outlined below.

2.1 BPL PROCESS STATION

There are two identical Bistable Processor and Logic (BPL) process stations located in separate Bistable/Coincidence Logic Cabinets (BCCs), PMS-JD-BCCB01 and PMS-JD-BCCB02. The BPLs receive input from process sensors, both analog and digital, and perform bistable functions, making the logical decision that the plant condition has exceeded pre-established limits. This includes, in the case of the over-temperature and over-power delta T channels, the computation of a setpoint value based on multiple process sensor inputs. Operational bypass logic, such as that applied to the source range Nuclear Instrumentation Subsystem (NIS) channels, is performed in the NIS process station.

Each BPL contains a single PM processor module that has two parts, a functional processor and a communications processor. The communications processor transmits the partial trip signals (bistable results) to the Local Coincidence Logic (LCL) process stations in every division. A single message is transmitted, and is electrically 'split' to go to the required destinations. The High Speed Link (HSL) connections to both LCLs in the same division are "copper" connections, while those going to other divisions are fiber optic, using transmit/receive modem pairs. The HSL connections are unidirectional. The functional processor part of the PM module scans the input modules, converts the process signals to engineering values (if not already done by the I/O modules), compares the values to setpoints (the bistable function) and passes the results to the communications processor for transmittal to the LCLs.

As part of the process value conversion function, the signals are validated. Signals that are outside of the valid range, or whose input module is determined to be failed by self-diagnostics, are set to 'BAD' quality. The bistable outputs associated with signals of 'BAD' quality are set to the tripped state and the bistable output signals are themselves given BAD quality. In addition to the bistable output value and the quality value, each bistable has two additional signals that can be manually set or removed via the Maintenance and Test Processor (MTP) console. These are the CHANNEL BYPASS signal and the FORCE PARTIAL TRIP signal. These are set independently for the two BPL process stations in the division. Resolution of the vector of bistable output values is performed by the processors of the LCL process station as described in Section 2.2.

A CI communications module in each BPL stores status information for transmission on the Advant Fieldbus 100 (AF100) bus. Operator actions made through the division's QDPS/Safety Display are

received from the AF100 bus via the CI communications module. This connection also provides for maintenance of the BPL software and setpoints from the MTP.

Sensor inputs are shared between the two BPL redundant process stations within a division. This sharing is done via a current loop connection or in the case of Resistance Temperature Detector (RTD) inputs a parallel connection. The sensor input values may be replaced by test injection signals, received via the AF100 bus, under control of a hardwired Test Enable keyswitch (digital) input and a test enable software signal also received via the AF100 bus. Injecting a signal in one BPL does not affect the use of that signal in the other BPL of the division.

Certain sensor signals are sent to the control system through analog isolation devices. These signals are used to regulate the primary process variables to keep them within the safety limits. The isolators prevent faults on the non-safety side from causing effects to the safety circuits that could prevent them from accomplishing their assigned safety functions. In the control system, signal validation techniques, such as median signal selection, are applied to reduce the multiple redundant measurements of each process parameter to a single value that best represent the process parameter.

2.2 LCL PROCESS STATION

There are two LCL process stations located in separate cabinets, the same as those that contain the BPL process stations. Each LCL receives eight HSLs containing the partial trip and partial actuation signals, one from each of the two BPLs in each of the four divisions. The process stations combine the partial trips via majority voting logic to actuate the reactor trip breakers in the division and combine the partial actuations to send system level Engineered Safety Feature (ESF) actuations to the component actuation logic performed in the Interposing Logic Cabinet (ILC) process stations.

Each LCL contains four PM processor modules, each of which has two parts, a functional processor and a communications processor. The communications processor is capable of receiving two HSLs (hence the need for four processors to handle the eight links) and of transmitting one HSL. The receive links are distributed among the four processors such that the two links from a given division are handled by different processors. Table 2-1 shows the LCL processor assignments. Note that in each LCL, two processors perform the reactor trip logic, one processor performs the ESF actuation logic, and one processor is only used for HSL communication.

The data received via HSL is shared between the four processors through the global memory segment of the CI. Each functional processor uses the two links it receives directly and the other six by way of the global memory. Each logical signal is resolved, on a point by point basis, according to the signal value, its quality, the CHANNEL BYPASS and FORCE PARTIAL TRIP states and the quality status of the HSL receiver channel over which the point is received. If a signal has BAD quality or if its receive channel has BAD quality then the signal from the other BPL is used. In the condition that signals of GOOD quality are available from both BPLs of a division, a logical OR of the FORCE PARTIAL TRIP OR SIGNAL VALUE AND NOT BYPASS is used. If both signals have BAD quality, then a default value, based on the preferred failure mode, which is TRUE for reactor trip actuations and FALSE for ESF actuations, is used. The resulting signals from the four divisions are passed on to the two out of four (2/4) or two out of three (2/3) voting logic.

Table 2-1 LCL Processor Assignments (Division B)			
LCL Station	**Processor Module**	**BPL TO LCL HSLs**	**Function of Processor**
LCL-1	PM1	DIV A BPL-1, DIV D BPL-2	Reactor trip DO
LCL-1	PM3	DIV B BPL-2, DIV C BPL-1	Reactor trip DO
LCL-1	PM2	DIV C BPL-2, DIV B BPL-1	ESF functions with HSL to ILC
LCL-1	PM4	DIV D BPL-1, DIV A BPL-2	HSL input only
LCL-2	PM2	DIV C BPL-2, DIV B BPL-1	Reactor trip DO
LCL-2	PM4	DIV D BPL-1, DIV A BPL-2	Reactor trip DO
LCL-2	PM1	DIV A BPL-1, DIV D BPL-2	ESF functions with HSL to ILC
LCL-2	PM3	DIV B BPL-2, DIV C BPL-1	HSL input only

Each of the reactor trip LCL processor modules generates two Reactor Trip (RT) signals, one for the undervoltage trip relay matrix and one for the shunt trip relay matrix. These signals are sent to the relay matrices via hard-wired outputs. Each processor module accesses a dedicated Digital Output (DO) relay output module to reduce the extent of lost functionality in the event of a single failure. The DO signals are combined with the contacts of the Watchdog Timer (WDT) to cause fail safe action upon failure of the processor. The trip relay matrices are discussed in further detail in Section 2.3.

A functional requirement of the PMS is that a Reactor Trip actuation shall be performed when the Safety Injection or Automatic Depressurization functions are initiated by either automatic or manual means. This feature is done by the LCL processor that performs ESF functions by sending a digital (software) signal to the two LCL processors performing reactor trip functions by way of the global memory feature of the CI module. The reactor trip functional processors then combine this signal with those from the BPL channel voting logic to generate the outputs sent to the trip interface matrix.

The logic signals received by the HSLs can be substituted with test injection signals, received via the AF100 bus, under control of the status of the Test Enable keyswitch (digital) input and a test enable software signal both of which are received via the AF100 bus. Only the enable signals from the LCL's own division are applied. Also, the digital output signals sent to the DO modules for reactor trip may be substituted for testing under the same controls.

Each LCL process station has an extension chassis that houses digital input modules. These digital input modules receive hardwired system level manual actuation signals from the Main Control Room (MCR) and from the Remote Shutdown Room (RSR). These digital input modules also receive the MCR/RSR transfer switch signals that allow control to be transferred to the RSR in the event of MCR evacuation. The manual reactor trip does not use the digital input modules; rather it is connected directly to the trip interface matrix, as is discussed in Section 2.3. Multiple digital input channels are used for each actuation function so that a single failure will neither prevent actuation of the division function at the system level nor cause spurious actuation of that function.

2.3 REACTOR TRIP INTERFACE

The interface between the LCL process stations and the reactor trip switchgear is described in Reference 1. One division is shown in Reference 1, but all four are identical.

2.4 ILC PROCESS STATION

The ILC process stations, located in the Interposing Logic Cabinets (ILC) implement the actuation of safety system equipment in response to the ESF system level commands generated in the LCL process stations. The system level signals are broken down to the individual actuation signals which actuate each component associated with a system-level engineered safety feature. For example, a single safeguards actuation signal must trip the reactor and the reactor coolant pumps, align core makeup tank valves and initiate containment isolation. The interposing logic accomplishes this function (with the exception of reactor trip). The power interface transforms the low level signals to voltages and currents needed to operate the actuation devices. The actuation devices, in turn, control motive power to the final engineered safety feature component.

The ILC cabinet contains redundant process stations, each receiving HSLs from the two LCL process stations that generate the system-level automatic commands. The two ILC process stations output the component actuation commands through separate DO channels which are combined on a Component Interface Module (CIM) for Air Operated Valve (AOV), Hydraulic Operated Valve (HOV), Motor Operated Valve (MOV), switchgear, and squib operated valves. The two ILC process stations use the hardwired port X inputs to the CIM. Configuration of the CIM determines whether the actuation logic is a logical OR of the two process stations, or a logical AND, depending on the need to prevent spurious actuations on single failures.

System level manual actuations are hardwired from switches in the MCR and in the RSR. These actuations are combined with the automatic actuations and are "fanned out" to the various components that are designated to act as a system. Thus the path to the ILC for both automatic and manual system level actuations uses the HSLs from the LCL process stations.

Onerous[1] component level manual commands originate in the QDPS/Safety Displays as soft controls. They are sent from the divisional QDPS/Safety Displays to the ILC process stations via the AF100 bus. The ILC combines the manual component commands with automatic demands from the LCLs and passes the result to the CIM modules via hardwired digital interface. The component level logic performed by the CIM provides command latching and command termination at end of travel.

Non-onerous component level manual commands originate in the Plant Control System (PLS) as soft control actions on the graphic displays. They are then sent via PLS remote I/O branches to the CIMs located in the ILC cabinets. The CIMs give priority to safety actuations of the plant equipment, but in the absence of safety actuations allow the normal manual operation of the equipment to be done. The

1. Onerous actuation is defined as that which causes a breach of the RCS pressure boundary or a need to shut down the plant to cold conditions to effect repairs.

component level logic performed by the CIM downstream of the priority logic provides command latching and command termination at end of travel. For motor operated valves, the motion is stopped on thermal overload conditions if the command origin was the non-safety system, however, if the actuation came from the safety system, this condition causes an alarm to be actuated and motion continues. The CIMs contain no processors and execute no code and will not be discussed in this analysis.

2.5 NIS PROCESS STATION

The Nuclear Instrumentation Subsystem (NIS), located in the Nuclear Instrumentation Cabinet (NIC) PMS-JD-NICB01, contains two redundant Common Q process stations NIS-B1 and NIS-B2; both being aligned with each of the BPL process stations discussed in Section 2.1. These process stations perform the special signal processing required for EX-CORE nuclear instrumentation channels and provide redundant processing capabilities should a process station (NIS-B1 or NIS-B2) become inoperable.

The Nuclear Instrumentation Modules (NIMODs), one for each range (source, wide and power), are also contained in the NIC cabinet. These modules are the special electronics needed to convert nuclear instrumentation signals into the standard input levels of digital protections systems. They include the high voltage power supplies necessary for neutron detectors. For a detailed description of the NIMODs refer to Reference 1, Section 2.5.

2.6 ICP PROCESS STATION

Each division of the PMS has an Interface Communication Processor (ICP) located in the same cabinet as the MTP and the Interface and Test Processor (ITP). The ICP gathers signals that will be used in the non-safety control systems and sends them through digital-to-analog converters and qualified isolators to the control cabinets. Signals are segmented into five groups with each group having its own analog output module so that if a failure occurs, only one group is affected. These segmentation groups correspond to the major control functions (e.g., reactor power control, steam generator level control, etc.) which are also segmented within the non-safety control system. A given signal may be present in multiple groups. Sensor signals that are 4-20 mA current loops are sent to the non-safety control system directly, through isolation devices, and do not pass through the ICP. ICP signals are those that are compensated or otherwise are calculated within the PMS.

In addition to the primary function of the ICP described above, each ICP is cross connected to its counterparts in the other divisions to allow signals to be shared for the purpose of display on the QDPS/Safety Displays (see Section 2.9). This permits all redundant measurements to be displayed side by side on each division's display where they can be compared by the operator.

Two processor modules are present in the ICP to receive the three HSLs from other divisions; however, no functional redundancy is performed between the two processors. The ICP process station contains a CI communications module to communicate with the other process stations in the division via the divisional AF100 network.

2.7 ITP PROCESS STATION

The ITP process station monitors the status of the division's cabinets and performs diagnostics that require information beyond that which is available in the individual processors and summarizes the diagnostic performed by the individual processors to activate a system trouble alarm when a problem is detected. The ITP process stations in the four divisions are interconnected via fiber optically isolated HSLs so that comparisons of sensor values can be made.

Two processor modules are present in the ITP to receive the three HSLs from other divisions; however, no functional redundancy is performed between the two processors. The ITP process station contains a CI communications module to communicate with the other process stations in the division via the divisional AF100 network.

Key-lock switches, located in the cabinet housing the ITP station, are scanned by digital input modules in the ITP process station. These switches enable test and maintenance functions to be performed, and are provided as a further level of access control (beyond the cabinet door locks) to support administrative control of these functions.

2.8 MTP PROCESS STATION

The MTP process station is located in the same cabinet as the ITP and ICP process stations. It provides local display of the division status, and provides the means to conduct surveillance testing of the division (typically done during plant shutdown) as well as software maintenance of the various processors within the division. It is through the MTP that the software is loaded into the division processors under control of a maintenance enable key lock switch.

The MTP consists of a Personal Computer (PC) node box and a Flat Panel Display (FPD) with associated keyboard. Both are qualified for application to the monitoring and maintenance functions of the PMS. The PC node box also contains an Ethernet interface module through which it connects to a gateway on the Real Time Data Network (RTDN). Through this gateway, the MTP provides information on system status and process measurements for display and historical recording to the Human System Interface (HSI). The network media between the MTP PC node box and the gateway workstation is fiber optic to provide the required electrical isolation.

2.9 QDPS/SAFETY DISPLAY SUBSYSTEM

Each of the four PMS divisions contains a QDPS/Safety Display located on the Dedicated Safety Panel (DSP) in the MCR. Each QDPS/Safety Display consists of a PC node box and a FPD unit. The PC node box is connected to the division AF100 network. All divisional process stations provide status information for display via the AF100 network.

Manual actuations of permissives, blocks, resets and system level resets are originated at the QDPS/Safety Display as soft controls. They are sent from the QDPS/Safety Display PC node box via the AF100 network to the BPL and LCL process stations in the division. In the receiving process station, the actuation commands are applied to the functional logic controlling the equipment as appropriate for the given manual command.

In addition to providing status and actuation of the PMS divisions, the QDPS/Safety Display panel provides the QDPS display information. Each QDPS/Safety Display indicates process variables required for monitoring and controlling the post event plant state. The process variables are defined by Regulatory Guide 1.97.

The operator makes display selections using a navigational device.

2.10 QDPS PROCESS STATION

The QDPS process stations read process measurements that are required for post accident monitoring, but are otherwise not required by the PMS for safety actuations. In addition, signals that are needed for both QDPS and safety actuations and that are required to be available up to 72 hours following the event are input to the QDPS process station. These latter signals are sent via shared current loop to the BCCs as well. This arrangement allows non-essential cabinets to be powered from the 24 hour batteries in the event of a total blackout.

There are two QDPS process stations, one in each of divisions B and C. Processed measurements are sent to all four QDPS/Safety Displays by way of the ICP process station inter-divisional HSL connections and the divisional AF100 networks (see Section 2.6). The division B and C QDPS process stations are also cross-connected via the HSLs (division B sends data to division C and vice versa). When relying on equipment powered from the 72 hour battery bus, the cross connection enables division B and C QDPS signals to be viewed on either QDPS/Safety Display in event of failure of one of the QDPS/Safety Displays.

a,c

Figure 2-1. PMS One Line Architecture

a,c

Figure 2-2. Typical PMS Division Configuration (Division B Shown)

3 SHA BASIS

1. The system is operating normal with no parameters bypassed when the single failure occurs.

2. Test logic does not prevent the system from performing its protective functions. That is, actual trip signals will override less conservative test signals.

3. The design is such that a loss of power or signal to a device that outputs trip/no-trip state information results in a reactor trip (RT) state to subsequent devices.

4. If bistable bypass information is lost to a processor, the processor uses the last known valid data for the bistable bypass state.

5. Communication between processors will be validated by the receiving processor and the data defaulted to a safe-state if necessary.

6. Hardware or "Protection" software common mode failures that affect the PMS system protective (safety critical) functions are mitigated by the DAS.

7. The primary method of detection for programming errors is verification and validation.

8. "Administrative Inspection" is to be Operator monitoring of the system status via DDS.

9. Verification and Validation includes code inspection.

4 SHA METHODOLOGY

This analysis uses results from the PMS FMEA as input to the SHA. A review of the current FMEA (Reference 1) was performed to identify processor module failure states (causes) which represent a potential hazard at the system level. This effort eliminates the hardware related hazardous states and identifies the processor modules whose software will be the starting point for these software hazards analysis.

The SHA includes the following steps:

1. Definition of the system to be analyzed
2. Construction of functional block diagrams
3. Identification of all potential software hazard failure modes
4. Evaluation of each hazard failure mode in terms of the worst potential consequences
5. Identification of the hazard failure detection methods and compensating provisions
6. Identification of corrective design or other actions to eliminate/control the hazard
7. Identification of impacts of the corrective change
8. Documenting the analysis and summarization of the hazards that could not be corrected

The analysis considers credible outputs from the system's computers (e.g., communications failures, CPU stalls, etc.). Not all possible causes of the failure are listed, as the intent is to show the plausibility of the suggested failure.

The FMEA confirms there are no single hardware failures that could lead to a hazardous condition. Only the PMS portion is further addressed herein.

During the software design implementation phase, the software architectural design will be reviewed for the introduction of any new additional unacceptable hazards. This review will be performed by postulating similar credible faults/failures and evaluating their effects on the results of this SHA.

The SHA contained in Section 5 is documented in tabular format and Table 4-1 below describes the column headings for the SHA matrix.

When the analysis identifies, "Program error or software failure," the intent is to describe a condition in which the operating system or application program within a given processor becomes corrupt in some manner. It is assumed that the program is initially correct, but because of a component failure, or some unknown external influence, the program is not the same program that was initially loaded.

When the analysis identifies, "System diagnostics," the test features of the PMS system automatically detects faults in the system. The system is designed to provide verification of complete system functionality using a combination of overlapping functional tests and System diagnostics. The functional tests are executed manually as needed using the MTP FPDs. The System diagnostics are automatically executed on a continuous basis and provide operator notification in the event of a failure. Taken together, these two types of testing provide a demonstration that the entire system is functioning properly.

Table 4-1 PMS SHA Matrix Column Headings	
Column	**Content**
Name	Descriptive name of the component.
Hazard Description	Identifies the postulated hazard failure mode of the component.
Hazard Cause	Probable cause(s) of the hazard.
Method of Detection	Lists possible means by which the failure may be detected
Potential Consequences	This column describes the effect that the failure has on the system as regards its ability to perform the safety function.
Safety Hazard Mitigation	This column describes what design features or actions are considered to mitigate the potential hazards.
Safety Hazard Control Verification Method	This column provides information how the Hazard Control Requirements are verified and/or validated, such as: document review, code inspection, software testing or system validation testing

5 SHA TABLES

Table 5-1 PMS Software Hazard Analysis Matrix

a,c

Table 5-1 (cont.) PMS Software Hazard Analysis Matrix

a,c

Table 5-1 (cont.) PMS Software Hazard Analysis Matrix

a,c

Table 5-1 (cont.) PMS Software Hazard Analysis Matrix

a,c

Table 5-1 (cont.) PMS Software Hazard Analysis Matrix

a,c

Table 5-1 (cont.) PMS Software Hazard Analysis Matrix

a,c

Table 5-1 (cont.) PMS Software Hazard Analysis Matrix

a,c

Table 5-1 (cont.) PMS Software Hazard Analysis Matrix

a,c

Table 5-1 (cont.) PMS Software Hazard Analysis Matrix

a,c

Table 5-1 (cont.) PMS Software Hazard Analysis Matrix

a,c

Table 5-1 (cont.) **PMS Software Hazard Analysis Matrix**

a,c

Table 5-1 (cont.) PMS Software Hazard Analysis Matrix

a,c

Table 5-1 (cont.) PMS Software Hazard Analysis Matrix

a,c

Table 5-1 (cont.) PMS Software Hazard Analysis Matrix

a,c

Table 5-1 (cont.) PMS Software Hazard Analysis Matrix

a,c

Table 5-1 (cont.) PMS Software Hazard Analysis Matrix

a,c

Table 5-1 (cont.) PMS Software Hazard Analysis Matrix

a,c

Table 5-1 (cont.) **PMS Software Hazard Analysis Matrix**

a,c

Table 5-1 (cont.) PMS Software Hazard Analysis Matrix

a,c

Table 5-1 (cont.) PMS Software Hazard Analysis Matrix

a,c

Name	Hazard Description	Hazard Cause	Method of Detection	Potential Consequences	Safety Hazard Mitigation	Safety Hazard Control Verification Method

Table 5-1 (cont.) PMS Software Hazard Analysis Matrix

a,c

Table 5-1 (cont.) PMS Software Hazard Analysis Matrix

a,c

Table 5-1 (cont.) PMS Software Hazard Analysis Matrix

a,c

Table 5-1 (cont.) PMS Software Hazard Analysis Matrix

a,c

Table 5-1 (cont.) PMS Software Hazard Analysis Matrix

a,c

Table 5-1 (cont.) PMS Software Hazard Analysis Matrix

a,c

Table 5-1 (cont.) PMS Software Hazard Analysis Matrix

a,c

Table 5-1 (cont.) PMS Software Hazard Analysis Matrix

a,c
