



ANP-10273NP
Revision 0

**AV42 Priority Actuation and Control Module
Topical Report**

November 2006

AREVA NP Inc.

Non-Proprietary

(c) 2006 AREVA NP Inc.

U.S. Nuclear Regulatory Commission

Disclaimer

Important Notice Concerning the Contents and Application of This Report

Please Read Carefully

This report was developed based on research and development funded and conducted by AREVA NP, Inc., and is being submitted by AREVA NP to the U.S. Nuclear Regulatory Commission (NRC) to facilitate future licensing processes that may be pursued by licensees or applicants that are customers of AREVA NP. The information contained in this report may be used by the NRC and, under the terms of applicable agreements with AREVA NP, those customers seeking licenses or license amendments to assist in demonstrating compliance with NRC regulations. The information provided in this report is true and correct to the best of AREVA NP's knowledge, information, and belief.

AREVA NP's warranties and representations concerning the content of this report are set forth in agreements between AREVA NP and individual customers. Except as otherwise expressly provided in such agreements with its customers, neither AREVA NP nor any person acting on behalf of AREVA NP:

- Makes any warranty or representation, expressed or implied, with respect to the accuracy, completeness, or usefulness of the information contained in this report, nor the use of any information, apparatus, method, or process disclosed in this report.
- Assumes any liability with respect to the use of or for damages resulting from the use of any information, apparatus, method, or process disclosed in this report.

ABSTRACT

This report describes the design features of selected signals from safety-related Class 1E main control room actuators, remote shutdown station actuators, safety-related Class 1E TELEPERM XS system outputs, and non-safety-related control actuations (i.e., signals). This includes the execute features for actuation and driver devices and the checkback signals from safety-related components. The AV42 is a priority and actuation control module that handles these signals and their interfaces.

The AV42 prioritizes the various command inputs and executes an output to plant components that reflects the plant licensing basis and operational preferences. In addition, it monitors checkback signals from the actuators and drives and provides these checkbacks to various instrumentation and control (I&C) systems. The AV42 module processes commands from all areas (e.g., inputs received from safety and non-safety-related instrumentation and control systems, the main control room and remote shutdown station).

The AV42 module is designed for use in any safety-related or non-safety-related system. The AV42 module complies with the appropriate NRC regulations and industry standards for safety-related systems. This report describes the design of the AV42 module and demonstrates how the AV42 module complies to Class 1E equipment design, qualification, and quality criteria as well as criteria for the prioritization of Engineered Safety Features Actuation System (ESFAS) signals and for the electrical separation and independence of redundant systems.

The AV42 module will be used in Class 1E circuits; therefore, it will be subject to periodic testing governed by Technical Specifications. This document describes those tests, including test coverage and overlaps. This document also describes the reliability data that has been used to establish the required testing frequency.

Nature of Changes

Item	Section(s) or Page(s)	Description and Justification
------	--------------------------	-------------------------------

Contents

	<u>Page</u>
1.0 EXECUTIVE SUMMARY	1-1
2.0 INTRODUCTION	2-1
3.0 LICENSING BASES.....	3-1
4.0 AV42 MODULE DESCRIPTION.....	4-1
4.1 General	4-1
4.2 Functions	4-1
4.3 Operation	4-4
4.4 Testing	4-5
4.5 Power Supplies	4-8
4.6 Implementation	4-9
4.7 Cyber Security	4-15
4.8 Independence of the AV42 Module.....	4-16
4.9 Configuration Management Plan	4-19
4.10 Maintenance Procedures	4-21
4.11 Anticipated Transient Without Scram.....	4-22
5.0 HARDWARE QUALITY	5-1
5.1 AV42 PLD Logic Quality	5-1
5.2 PROFIBUS [®] Controller	5-4
6.0 QUALIFICATION ANALYSIS	6-1
6.1 Environmental, Electrical, Seismic, EMC, ESD TESTING and Radiation Analysis	6-1
6.2 Environmental.....	6-1
6.3 Electrical	6-3
6.4 Seismic	6-5
6.5 EMC/ESD	6-6
6.6 Radiation.....	6-10
7.0 RELIABILITY	7-1
7.1 Failure Modes and Effects Analysis.....	7-1
7.2 Failure Rate Analysis	7-1
7.3 Operating History	7-2
8.0 CONCLUSIONS	8-1
9.0 REFERENCES	9-1

Tables

Page

Table 4-1 AV42 Priority Actuation And Control Example..... 4-12

Figures

Figure 4-1 AV42 Interfaces And Communication Links 4-5
Figure 4-2 Overlap Testing..... 4-6
Figure 4-3 AV42 Module Application 4-10
Figure 4-4 Priority Actuation And Control Logic Example..... 4-14

Nomenclature

Acronym	Definition
°C	Degrees Celsius
°F	Degrees Fahrenheit
AC	Alternating Current
ANSI	American National Standards Institute
AP	Automation Processor
ASIC	Application Specific Integrated Circuit
ASME	American Society of Mechanical Engineers
ASP	Auxiliary Shutdown Panel
ATWS	Anticipated Transients Without Scram
AV42	AREVA NP's Priority and Actuation Control Module
BTP	Branch Technical Position
CBSFTOFF	AV42 Checkback Output Status-OFF
CBSFTON	AV42 Checkback Output Status-ON
CFR	Code of Federal Regulations
CM	Configuration Management
DC	Direct Current
dB	Decibel
DIN	German Institute for Standards
EAS	Essential Auxiliary Systems
EEPROM	Electrical Erasable Programmable Read Only Memory
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
EPRI	Electric Power Research Institute
ESD	Electro Static Discharge
ESF	Engineered Safety Feature
ESFAS	Engineered Safety Features Actuation System
FDFLT	Feeder Fault Signal
FMEA	Failure Modes and Effects Analysis
GDC	General Design Criteria
GHz	Gigahertz
Hz	Hertz
HICB	Human, Instrumentation and Controls Branch (Currently EICA)
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronic Engineers
I/O	Input/Output
I&C	Instrumentation and Control
KTA	German Nuclear Safety Standards Commission
kHz	Kilohertz
kV	Kilovolt
LED	Light Emitting Diode
MAX	Multiple Array Matrix

MCC	Motor Control Circuit
MCR	Main Control Room
MHz	Megahertz
MTBF	Mean Time Between Failures
NRC	Nuclear Regulatory Commission
OBE	Operating Basis Earthquake
OLM	Optical Link Module
OM690	Screen-based TXP Operation and Monitoring System
OPDIS	Operation Disable
PAC	Priority Actuation and Control
PLD	Programmable Logic Device
QA	Quality Assurance
rad	Radiation Absorbed Dose
RF	Radio Frequency
RFI	Radio Frequency Interference
RPS	Reactor Protection System
RSS	Remote Shutdown Station
RTS	Reactor Trip System
SER	Safety Evaluation Report
SFTIN	AV42 Test Input
SSE	Safe Shutdown Earthquake
TR	Technical Report
TXP	TELEPERM XP System
TXS	TELEPERM XS System
TUEV	Technischer Ueberwachungs Verein (German Technical Surveillance Association)
U.S. EPR	AREVA NP's Evolutionary Power Reactor
V	Volt
VDC	Volts Direct Current
V/m	Volts/Meter

1.0 EXECUTIVE SUMMARY

This report describes the design features of the AREVA NP AV42 Priority Actuation and Control (PAC) Module. The AV42 prioritizes the various command input signals from safety-related Class 1E main control room actuators, remote shutdown station actuators, safety-related Class 1E TELEPERM XS (TXS) system outputs, and non-safety-related controls and outputs to plant components. In addition, it monitors checkback signals from the actuators and drivers and provides these checkbacks to various instrumentation and control systems. The AV42 module is designed for use in both safety-related or non-safety-related systems.

The AV42 module complies with the appropriate NRC regulations and industry standards for safety-related systems. This report describes the design of the AV42 module and demonstrates AV42 module compliance to Class 1E equipment design, qualification, and quality criteria as well as criteria for the prioritization of safety-related signals and for the electrical separation and independence of redundant systems.

AREVA NP requests that the Nuclear Regulatory Commission (NRC) issue a Safety Evaluation Report (SER) that approves the use of the AV42 module as described in the topical report. The AV42 module will be used in the AREVA NP's Evolutionary Power Reactor (U.S. EPR) design. AREVA NP plans to reference the approved version of the topical report in its Design Control Document for the U.S. EPR. AREVA NP also expects that the AV42 module will be used in future I&C modernization projects at operating nuclear plants.

2.0 INTRODUCTION

This document discusses the use of the TXS AV42 module. The AV42 module is a Class 1E safety-related device that can be used for both safety-related and non-safety-related instrumentation and control applications and is compatible with several types of input and output devices. This document provides the hardware design and licensing bases for the sense and command signal interface between safety-related manual controls of the main control room (MCR) and remote shutdown station (RSS), TXS safety-related command outputs, non-safety-related control command signals (e.g., TELEPERM XP System (TXP) automation processor (AP), OM690 and Simatic S7 systems), and the execute feature for actuation and driver devices to the safety-related components by using the AV42 priority actuation and control module.

The AV42 monitors and controls safety-related actuators and drives; however, it can also control non-safety-related actuation devices. The AV42 prioritizes the various sense and command inputs and executes an output that reflects the plant licensing requirements and operational preferences. In addition, it monitors the checkback signals from the actuators and drives and takes the appropriate action. Each actuator or drive to be controlled requires one AV42 module. The AV42 can process commands from all areas (e.g., inputs received from safety-related and non-safety-related instrumentation and control systems, automatic and manual portions of systems, and the main control room and remote shutdown panels).

The AV42 has two major components. The programmable logic device (PLD) is the first major component and consists of interconnected logic gate arrays. The second major component is an application specific integrated circuit (ASIC) PROFIBUS[®] controller and is safety-related for hardware qualification purposes; however, the functional capability and information and data flow of the ASIC PROFIBUS[®] is non-safety-related. The AV42 module operates during all modes of plant operation that utilize safety-related equipment that is actuated via the AV42, including normal conditions, test conditions, accident, post-accident, and severe accident conditions.

The following sections of this report discuss the design capabilities and the licensing bases met by the AV42. Section 3 presents the licensing bases for the design of the AV42 module and

demonstrates that the AV42 module is a safety-related device that can be used to actuate safety-related functions (e.g., the engineered safety features (ESF) and essential auxiliary systems (EAS)). The AV42 meets the regulations and follows the guidance presented in the NRC Standard Review Plan, NUREG-0800 Chapter 7 (Reference 18). Section 3 presents both the NRC regulations and industry standards along with special features of the AV42 module that require more detailed discussion concerning the licensing bases. Section 3 also presents the actuation priorities for the AV42 design and explains how they comply with regulatory requirements. The prioritization of safety-related automatic and manual signals supports safe plant operation. The design meets the manual and automatic actuation provisions of Institute of Electrical and Electronic Engineers (IEEE) 603 (Reference 28) and Regulatory Guide 1.62 (Reference 12).

Section 4 describes the as-built AV42 module generic design and explains the logic circuits, including the internal logic circuits for selecting the priority of the different input command signals. Examples of priorities that can be implemented at nuclear plants are provided. The testing and monitoring capabilities of the AV42 are presented. Particular attention is given to the separation and independence between safety-related hardware devices, including the logic design and information flow, and non-safety-related devices, including information flow. [

] Finally, the role of the AV42 module in the anticipated transients without scram (ATWS) mitigation system, configuration management (CM) plans, and maintenance procedures for the AV42 are summarized.

Section 5 presents the quality process used in the manufacturing, design, and testing of the AV42 module. [

]

Section 6 discusses the qualification of the AV42 module. Because it is part of the TXS family of devices, the qualification of the AV42 is similar to that for the TXS Instrumentation and Control (I&C) system. It includes the environmental and seismic qualification characteristics as

well as the electromagnetic compatibility (EMC) properties of the module. It includes the electrical properties of the module and power supply testing as well as a radiation analysis.

Section 7 presents reliability information for the AV42 module. It includes a discussion of a failure mode and effects analysis for systems containing the AV42 module, the operating history, and reliability calculations. Reliability calculations are used as the basis for performing required Technical Specification surveillances at refueling intervals of 18 or 24 months.

Section 8, the conclusion, provides results of the licensing assessment of the AV42 priority and actuation control module.

3.0 LICENSING BASES

The AV42 prioritizes safety-related and non-safety-related command inputs for the control of a safety-related actuation device. The AV42 can also control non-safety-related actuators and drivers. However, the AV42 primarily controls safety-related actuation devices using both safety and non-safety-related inputs.

Because the AV42 module will be used in safety-related systems including engineered safety features actuation systems (ESFAS), its design is required to meet applicable regulations and follow applicable industry guidance. The AV42 design meets the applicable requirements of NRC General Design Criteria (GDC) 1, 2, 4, 5, 10, 12, 13, 15, 17, 18, 19, 20, 21, 22, 23, 24, 25, and 29 (Reference 6), 10 CFR 50.55a (Reference 3), 10 CFR 50.55a(h) (Reference 4), and Appendix B of 10 CFR Part 50 (Reference 7). Section 9.0, References, lists all applicable U.S. regulations and NRC regulatory guidance documents.

All regulations noted above and all I&C standards pertaining to the design of safety-related systems, including ESFAS and EAS, are applicable to the AV42. IEEE 279 (Reference 22) and IEEE 603 contain requirements endorsed by 10 CFR 50.55a(h). Among these requirements are:

- Safety System Criteria
- Single Failure Criterion
- Completion of Protective Action
- Quality of Components and Modules
- Equipment Qualification
- System and Channel Integrity
- Independence Testing
- Information Displays
- Control of Access and Security
- Repair
- Identification
- Auxiliary Features
- Human Factors Considerations

- Reliability.

In addition, the requirements for Section 7.3 as well as the requirements for manual control from Sections 6.2 and 7.2 of IEEE 603 were considered during the design of the AV42. Section 4.3 discusses the capability for testing and calibration considered during the design. These requirements were all considered and are met by the AV42 design. These requirements provide high-level design criteria for the control and protection system interaction. Section 9.0, References, lists applicable U.S. and international industry standards.

The key design and licensing points examined for the implementation of the AV42 module include the independence between safety-related and non-safety-related functions and data and the independence between safety-related hardware and non-safety-related hardware, as discussed in GDC 24 and Section 6.3 of IEEE 603. Sections 4.5 and 4.7 discuss the requirements for these two areas.

The AV42 design and testing procedures ensure the logic design quality, which is a critical area. Section 5.1 discusses logic design quality.

Section 6 discusses the environmental qualification including Electromagnetic Interference (EMI) and Radio Frequency Interference (RFI) and radiation qualification. Section 6 also includes seismic and power supply testing.

4.0 AV42 MODULE DESCRIPTION

4.1 General

The AV42 is part of the TXS safety-related instrumentation and control system product line.

The AV42 receives automatic and manual commands from both non-safety-related (e.g., TXP AP, OM690 and Simatic S7) and safety-related (e.g., TXS and system and component manual) sources. The AV42 is designed and qualified as a safety-related device.

4.2 Functions

The AV42 connects the TXS platform, OM690, and TXP AP platform to plant actuation devices and control circuits. In addition to providing a path for automatic safety actuation capability from TXS, the AV42 can control either safety-related or non-safety-related actuators and drivers that can be controlled by the TXP OM690 and TXP AP or the existing safety-related manual actuators in either the main control room or on the RSS panel.

The AV42 design meets the manual and automatic actuation requirements of both IEEE 279 and IEEE 603 and the guidance provided in Regulatory Guide 1.62. Moreover, the AV42 priority actuation and control design provides a manual actuation capability that meets the guidance found in Branch Technical Position (BTP) Human, Instrumentation and Controls Branch (HICB)-19 (Reference 20) for diverse and independent manual actuation capability from the TXS-based automatic actuations.

The AV42 module performs the function of the drive control for safety-related actuators and drives, gives the commands from the TXS safety-related instrumentation, and controls the priority over the non-safety-related control commands. Every priority-controlled device uses one AV42 module. Therefore, the module only controls one drive or actuator. It also serves as the interface between the safety-related and operational (i.e., non-safety-related) commands to the safety-related drivers:

The AV42 module can be used to control the following types of actuators and drives:

- Solenoid valves
- Motors for various components (e.g., pumps and fans)
- "Open-Loop" controlled actuators for various components (e.g., isolation valves and plug valves)
- "Closed-Loop" controlled actuators for control valves.

The priority and actuation control function of the AV42 module performs the following functions:

- Prioritization of actuation requests
- Drive actuation
- Drive monitoring
- Component protection
- MCR-RSS selection.

The following safety-related functions are implemented in the PLD:

- Safety-related command acquisition and prioritization

- Acquisition and processing of the checkback signals from the actuators and the switchgear
- Command output and command termination
- Lamp tests for I&C panels, MCR, or RSS.

The TXS-based safety-related I&C systems issue safety-related control commands over hardwired connections. The safety-related manual system level commands are hardwired to the AV42 from switches in the MCR and RSS. The command that designates the MCR or RSS and provides for command capability from a location that meets the requirements of 10 CFR 50.48 (Reference 1) and 10 CFR Part 50 Appendix R (Reference 8) is another safety-related hardwired



The non-safety-related control commands cover all automatic commands from the TXP AP operational I&C and manual commands from hand switches, appropriately isolated hardwired inputs from other non-safety related I&C systems, the Simatic S7 system, or the OM690 system. It does not cover the manual commands important to safety, which can also be issued from the MCR.

The controller implements only non-safety-related functions of the AV42. The controller is equipped to process the following functions:





4.3 Operation

The type of actuator and the desired actuator control signals, including the command termination signals that align with the indication and signaling functions, are derived from the specific application functional requirements. Other design inputs considered for a specific application are the operation capability from the OM690 screen-based soft controls and the number of connections to safety signals. Figure 4-1 below shows the principal structure, interfaces, and integration of the AV42 into the systems as well as the priority commands for actuations and drives, which receive commands from the safety-related TXS instrumentation and control





Figure 4-1 AV42 Interfaces and Communication Links

4.4 Testing

The testing configuration of the AV42 follows the guidance provided in Regulatory Guides 1.118 (Reference 16) and 1.22 (Reference 9). In addition, the testing provisions of IEEE 338 (Reference 24) have been followed. The overall I&C system design including the AV42 follows the guidance presented in Regulatory Guide 1.47 (Reference 10).

The testing of the AV42 confirms whether commands from the TXS are received correctly and whether they have the required priority over the control commands. GO and NO-GO tests are manually initiated periodically to form overlapping tests. In the course of the overlap testing for the safety I&C systems, including the AV42, each actuator is checked for the receipt and execution of safety I&C commands. This overlap testing checks the output of the safety signal, the integrity of the leads, and the priority operability of the AV42.

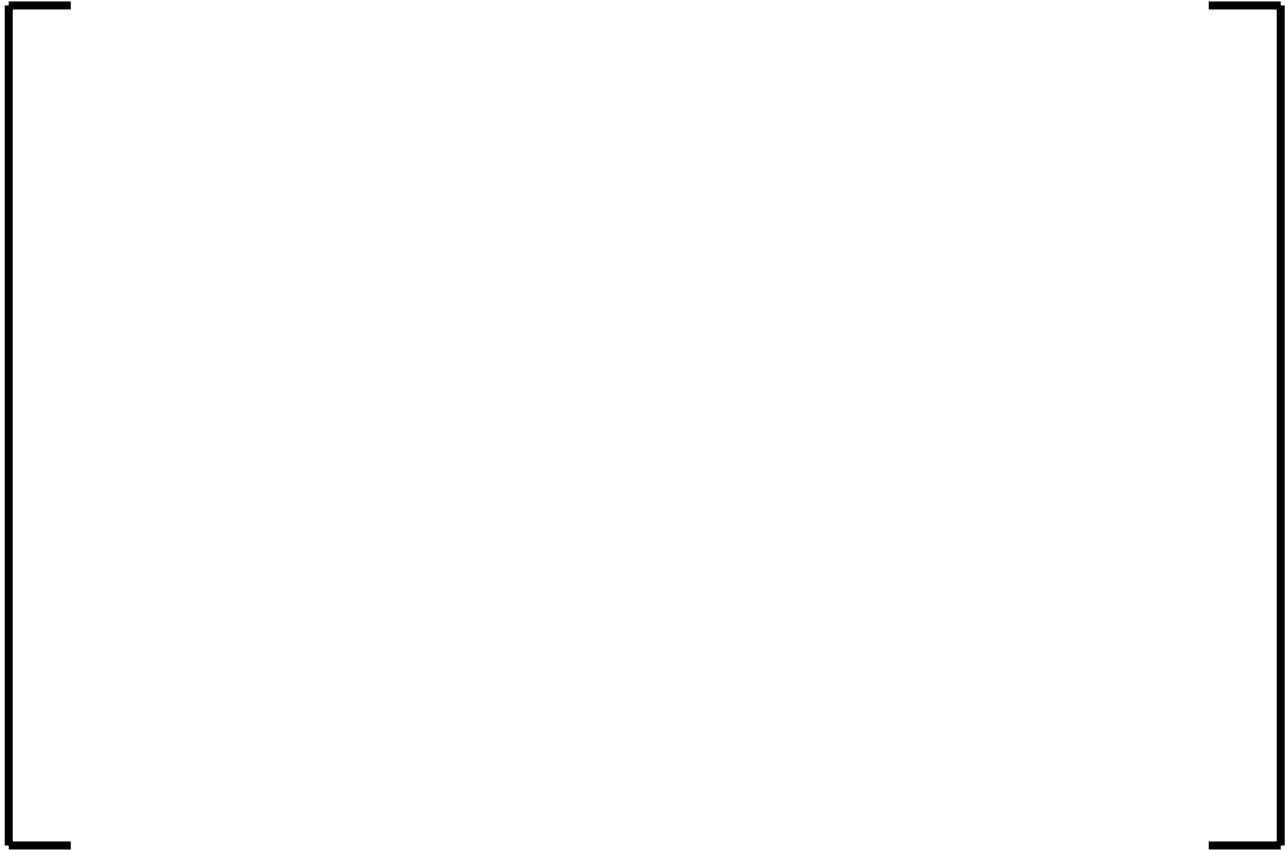


Figure 4-2 Overlap Testing






The AV42 monitors for open-and short-circuits and monitors module power supply for undervoltage. If there is a short circuit or an overload on the driver circuits, the status signal is activated. The PLD evaluates the status and forwards a fault message to the controller for further processing and transmittal via the multiplexer.

The AV42 can implement the testing of the lamps on the reactor protection system (RPS) or ESFAS local panels and the MCR or RSS. After the test signal is acquired by the PLD, the testing for the alarm lamps on the reactor protection panel begins.

The two lines that output commands to the switchgear are monitored for an open-circuit condition when in the de-energized state. This monitoring occurs through the coils of the interposing relays. The feeder fault signal (FDFLT) signal contains a fault message for an open-circuit condition.

The light emitting diodes (LED's) on the front plate of the AV42 indicate the operating status and the position of the controlled actuation device. The LED light configuration aids in the troubleshooting of the module by illuminating different patterns for the different situations (e.g., fault free operation, start up fault, or operational fault). The outputs of the AV42 route messages to the indications on the TXP screen-based soft controls. Such information as motion direction, position, checkback faults, voltage, action blocking, or runtime fault can be displayed.



The response time of the AV42 module is included in the total system response time calculations so that the AV42 module ensures that plant response time requirements for each specific application continue to be met. Because the safety functional path of the PLD design consists of only logic gates, gradual response time degradation is not credible. The only failure that could affect response time is a catastrophic failure, which is readily detectable through other types of surveillances. For example, plant specific functional testing or calibrations are sufficient to determine the proper functionality and acceptable operability, including acceptable response time for the AV42. Therefore, no periodic surveillances to check the AV42 response time degradation are required.

4.5 Power Supplies

The AV42 power supply and the alarm signal power supply used for fault messages are required for operation of the AV42 module. The power supplies for the AV42 connect to the safety-related power sources of the actuated systems through the normal TXS I&C system configuration. Both power supply inputs have their own protection circuit that protects against

transient over-voltage, polarity reversal, and overload due to short circuits within the circuits of the AV42 module. When the fault is removed, the power supply automatically resets automatically when the AV42 is powered on.

The power source conforms to the qualification guidance as described in Section 4.6 of Electric Power Research Institute (EPRI) Technical Report (TR)-107330 (Reference 33) and meets the power requirements of Section 8 of IEEE 603.

4.6 Implementation

Depending on the functional requirements and the intended scope of changes, the AV42 module can be implemented different ways in the control circuits of actuators. Figure 4-3 below shows a possible application scheme of the AV42 module.



Figure 4-3 AV42 Module Application



The AV42 operates in cooperation with the TXS to automatically process safety-related commands with a high reliability for the range of conditions specified. The manual control commands are designed to not defeat any of the requirements of the safety-related automatic actuations. Manual controls enable the operator to initiate protective actions at the system level as well as the individual component level. Manual operator actions and the number of discrete components necessary to perform these actions are minimized. The AV42 Module is designed and tested to confirm that the components as a whole demonstrate acceptable module

performance to ensure the completion of protective actions over the range of accident, transient, and steady-state conditions for a plant. Necessary manual actions can be taken to maintain safe conditions after the protective actions are completed.



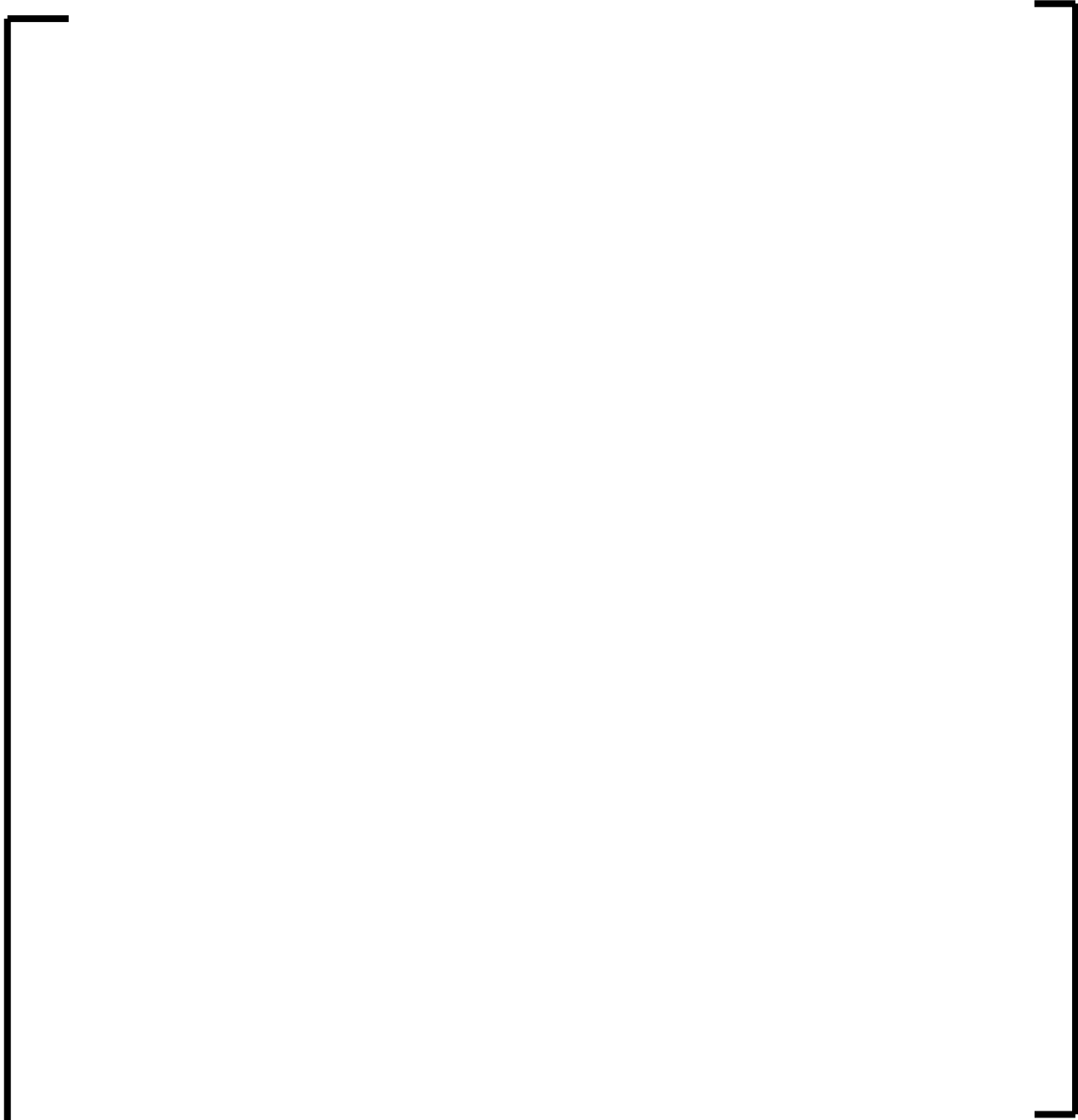
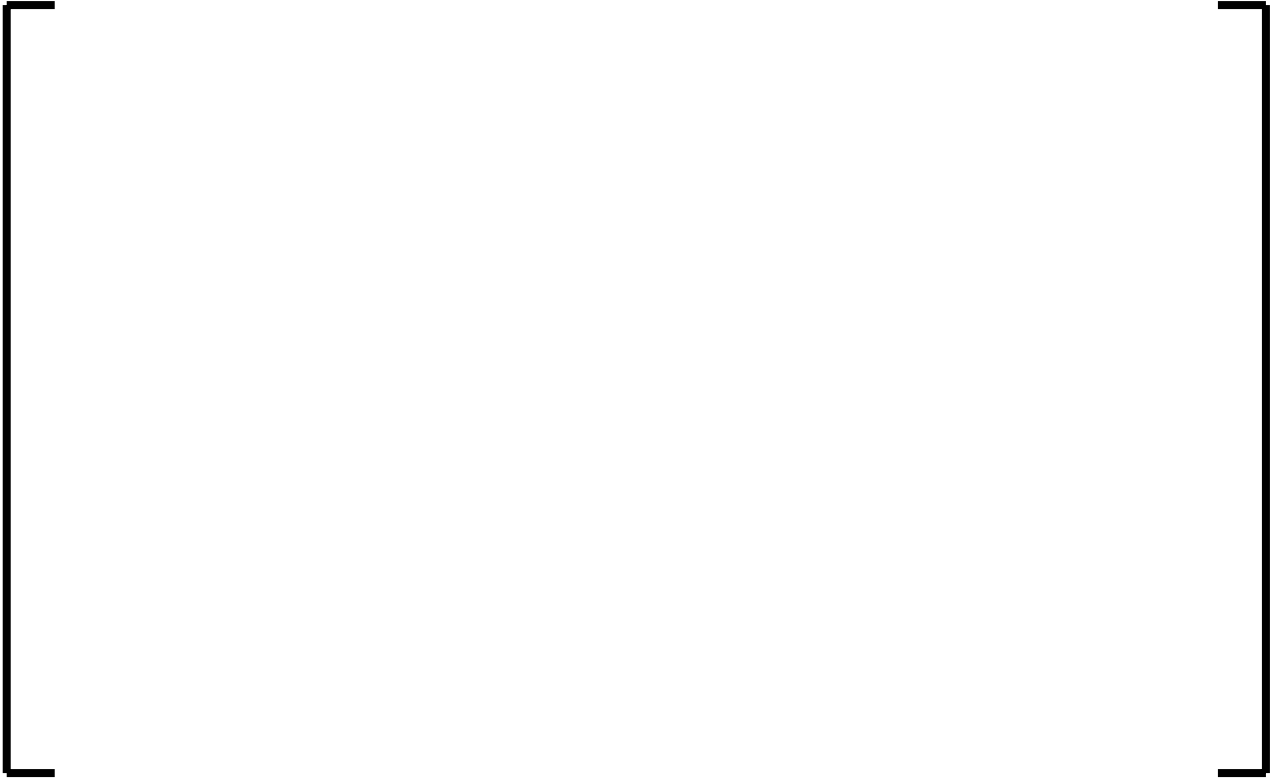


Table 4-1 AV42 Priority Actuation and Control Example

The checkback signals from the actuators are used for internal logic interlocks. This means that a valve open command is reset when the full open position limit switch of the actuators is triggered. Also, the torque limit switches are used in the switch off logic. For the start of the actuator, the torque limit switch interlock is disabled so that the actuator can be provided with a



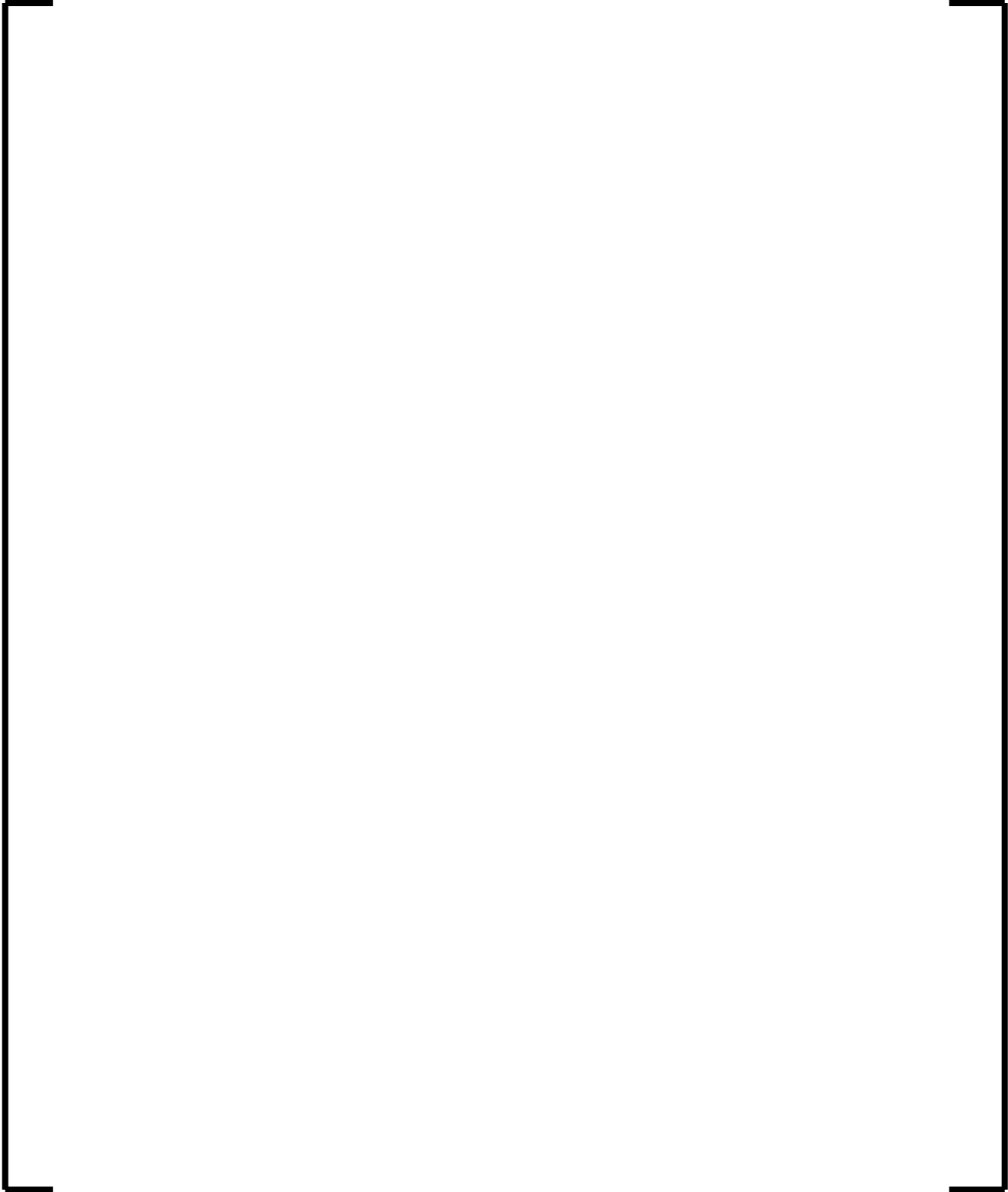


Figure 4-4 - Priority Actuation and Control Logic Example

In this example:



4.7 Cyber Security

Cyber security threats to the AV42 have been evaluated and determined not to be credible. AREVA NP and plant specific methods and strategies for managing an effective cyber security program are sufficient to prevent these threats from occurring to the AV42. Front and rear mounted cabinet doors control access to the AV42 hardware. Access to the AV42 hardware is controlled during normal operation. Because of the design and control of the AV42, storage media, communications, tests, and maintenance threat categories are highly improbable.

Examples of plant specific control include the layers of physical protection within the plant (e.g., owner controlled area, protected area, MCR alarms, and vital areas). Unescorted access to the AV42 area is restricted to authorized personnel. Visitors are to be escorted under direct control. Key carded locked barriers further restrict access to the AV42 area. Outsiders are denied



PROFIBUS® controller. Design information is classified as proprietary and is not publicly available, which further limits outside access.



Since the PLD contains only logic gate arrays, there is no opportunity for cyber security threats (e.g., a virus causing online modifications to an operating system or to any software). Because there are no outside communication links that can alter the logic gate arrays, the safety-related portion of the AV42 is protected from outside communication means. A security plan, training, work permits, and user authentication are extended to the AV42 to prevent unauthorized changes to hardware or configurations to limit cyber security threats for this area during maintenance, calibration, and other test activities

The inherent features of the AV42 design prevent unauthorized, undesirable, and unsafe intrusions throughout its life-cycle. These security features are part of the AV42 design and will meet the security requirements of the licensee as long as the system is installed and maintained in accordance with the plant administrative procedures and the licensee's security program.

4.8 Independence of the AV42 Module

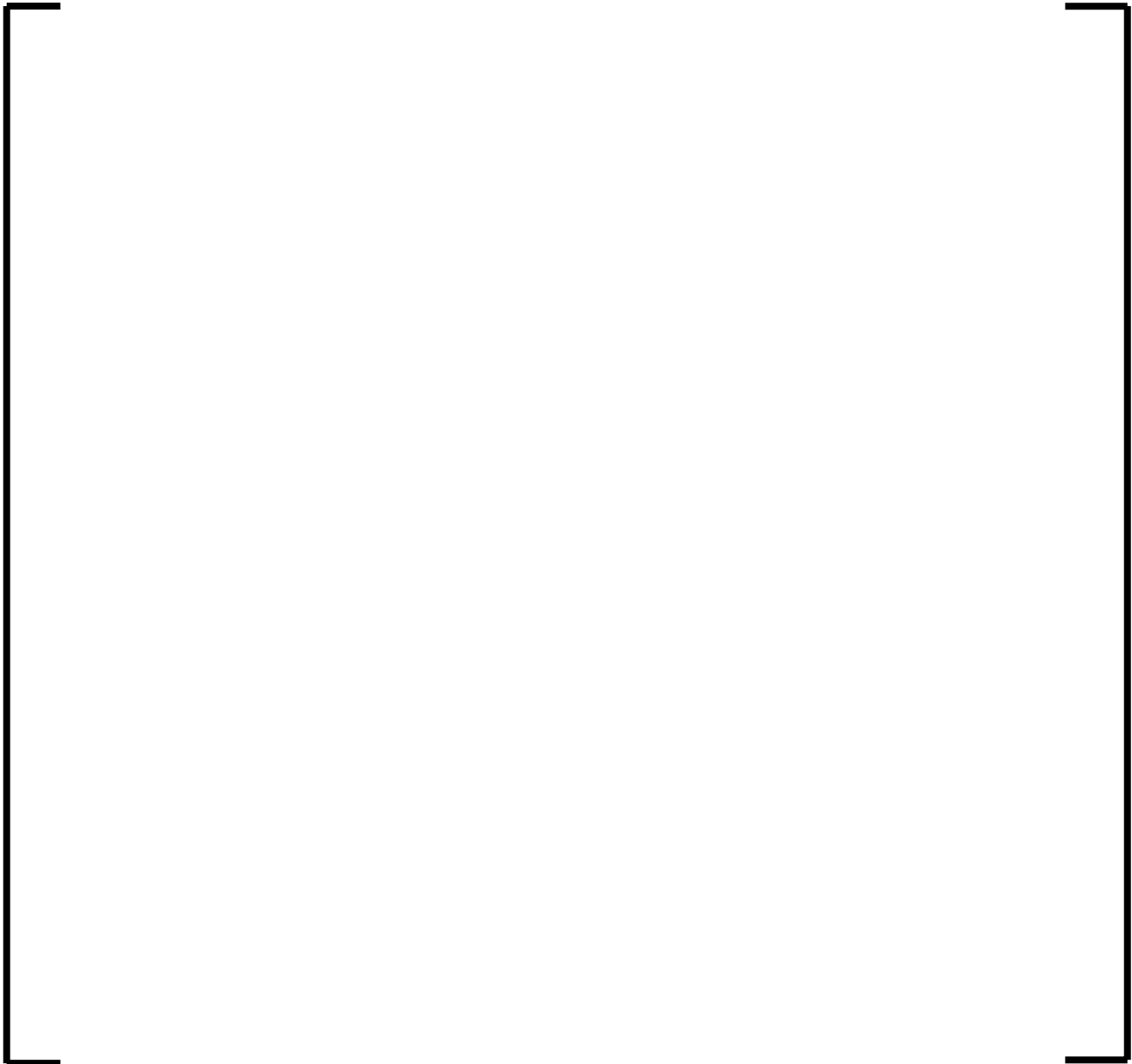
GDC 24 requires that the protection system, the AV42 module in this case, shall be separated from control systems to the extent that the failure of any single control system component or channel or the failure or removal of any AV42 component or channel from service which is common to the control and AV42 module leaves intact an AV42 module that satisfies all reliability, redundancy, and independence requirements.

Several methods are used to ensure the separation and independence of the non-safety-related circuits from the safety-related circuits and the independence between redundant safety-related circuits:

- Physical separation
- Electrical isolation
- Data flow separation

- Program and function flow separation

These separation methods are chosen so that the worst-case internal hazards or design basis events will not impair the capability of the safety functions of the AV42 module. The distances for physical separation follow the guidance of Regulatory Guide 1.75 (Reference 13) and IEEE 384 (Reference 27). Fiber optic cables between the AV42 and the various control systems provide the electrical isolation.



AREVA NP performed functional testing, which concluded that a faulted signal from any non-safety-related input cannot cause an error or a failure of any safety-related function of the AV42. The data flow from the controller cannot influence the safety functions of the AV42.

The design of the safety-related and non-safety-related interface within the PLD prevents the non-safety-related data from affecting the safety-related information and functions of the PLD. The fiber optic electrical isolation design and the isolation established by the inherent buffering of the PLD logic gate arrays meets the separation and independence requirements of GDC 24. The design of the PLD meets the separation, isolation, and independence requirements of IEEE 279 and Section 6.3 of IEEE 603. Any hardware or data failure of a non-safety-related data function or component does not affect the performance of the AV42 safety function. The safety function does not require input from the controller to perform the safety function.

4.9 Configuration Management Plan

Since its inception, the AV42 design has undergone configuration and change control. Each change to the AV42 must be independently assessed to confirm the qualification of the new version. A report is also issued for every version and identifies the valid documents and the components, hardware, and priority logic design. Configuration identification is applied to the priority logic and application specific configuration and associated documentation. The configuration of the AV42 module consists of the application specific embedded elements and the associated documentation.

The label of each configuration item is unique. The AV42 can be identified by a base identifier and an index. Both of these identifiers are written on the front plate of the AV42. A version number is assigned to each configuration item. Baselines are established for the control of design, product, and engineering changes.

The procedure to change configuration items consists of the following steps:

1. Submit change request
2. Evaluate the change request
3. Propose how to perform the change

4. Decide whether to implement the change
5. Perform the changes, including testing and updating the documentation.

The priority logic CM and change control applies to all documents and code. Control is affected through the implementation of the configuration identification, the change control, and status accounting functions. A formal change request initiates the change control process. A change request includes the following information:

- Identification of the request, product, date, and author
- Specification of the request, including the reason
- Identification of the configuration item
- Category of the request
- Current behavior of the product
- Requested behavior of the product.

Change requests are analyzed and evaluated, which results in the generation of a formal change proposal. This proposal provides the methodologies of performing the changes and the associated consequences. The change request forms the basis for the decisions taken by project management. A development order documents the decision. After the development, testing, and updating of the product-related documents, a formal document (product information) completes the change process and contains a summary report about the changed configuration item.

The measures described apply to the hardware, including the logic gate design of the PLD, and ensure that each application project is based on a qualified and well-configured set of building blocks of the system.

The project specific CM activities are supported by several unique activities. These activities are divided into two task groups:

- Ensure that only qualified hardware, logic development, and the logic interconnection design and components of the system are used (versions, releases).
- Ensure that the logic interconnection design is consistent with the application specific requirements.

The hardware configuration includes the revision to the module level, configuration of the underlying hardware components, and all manufacturers' documentation. The module level configuration includes a method for the identification of each major component so that changes can be tracked and evaluated for consistency with the AV42 design. The scope of the CM program consists of the creation and revision level of the design being used. All documentation associated with the AV42 development is also placed under the AREVA NP CM program.

AREVA NP has provided a structured method for CM that complies with regulatory guidance and requirements. For high quality designs, the CM process emphasis is on the importance of the design basis and associated design process information. The CM procedures reflect the need for a robust change management process and identification of versions.

4.10 Maintenance Procedures

The maintenance needs of the AV42 module are addressed in the same manner as those for the TXS system. The diagnostics and the testability of the AV42 provide the mechanisms needed to support maintenance at the module level. The AV42 has the same features as the TXS system that aid in module replacement. The maintenance manual contains a description of the hardware configuration for each module. Each cyclically sent dataset on the PROFIBUS[®] contains a unique identification of the AV42. If this identification deviates from the corresponding parameter in the flash memory of the module, a new parameter message is requested, and no operation commands are issued. Safety-related commands are not affected. This feature prevents the replacement of an AV42 with an incorrect parameter configuration.

The method of module hold-down is easily accessible and provides for the ease of module removal and reinstallation. These features also support calibration and post-installation testing. The AV42 manuals contain the information that is necessary to support preventive and corrective maintenance for all modules, including the power supplies, grounding features, and terminations.

The AV42 design includes many features that detect both hardware and PLD logic faults and assist in diagnostic and repair activities. If a bypass is implemented for any reason, the plant

specific design provides a bypass indication to alert operators to this condition. The AV42 bypass design conforms to the guidance in Regulatory Guide 1.47.

4.11 Anticipated Transient Without Scram

For ATWS implementation, one AV42 prioritizes both the inputs from both the safety-related ESFAS and the non-safety-related ATWS system, which occurs for the components actuated by both the ESFAS and the ATWS system. Individual plant specific applications will vary, but normally, the priority ranking places the safety-related ESFAS input higher than the non-safety-related ATWS input. The setting of the trip setpoints typically governs which system actuates first. The placement of the setpoints shall be in accordance with the requirements of 10 CFR 50.62 (Reference 5) so that the ESFAS actuation will always occur first unless subject to failure.

10 CFR 50.62 requires equipment from the sensor output to the final actuation device that is diverse and independent from the Reactor Trip System (RTS), to automatically initiate or trip the required systems and equipment under conditions indicative of an ATWS.



5.0 HARDWARE QUALITY

Hardware quality is ensured in the same manner as the same quality enhanced program used for the hardware qualification of the TXS instrumentation and control system. The quality program complies with 10 CFR 50.55a, Appendix B of 10 CFR Part 50, and American National Standards Institute (ANSI)/ American Society of Mechanical Engineers (ASME) NQA-1 (Reference 21). The AV42 also meets the high level quality requirements in 10 CFR 50.55a(h) and GDC 1 and 29. The NRC previously reviewed and approved the TXS quality program and reported the results of the review in a SER dated May 5, 2000 (Reference 46). Licensing Topical Report EMF-2110 (Reference 50) discusses the qualification process for the TXS system. The NRC approved this report and issued a SER.

Type test certificates document the actual qualification of the AV42. The type test is considered to be a form of generic product qualification. With the type test, all identical components are assumed to fulfill the quality provisions established for the AV42 hardware and are commensurate with the quality provisions of Appendix B of 10 CFR Part 50. The type test includes the evaluation of the component manufacturing process and the quality assurance (QA) system of AREVA NP. An independent party verified that the module conforms to all documentation. A general visual inspection was performed to determine the cleanliness, correctness of soldered joints, positioning of components, and electrical safety. Air and creepage distances were examined for the AV42 module. A third party review (TUEV) and in-house audits verified the proper implementation of the AREVA NP QA process for the AV42. All safety-related system properties were certified through the component type-tests and the integration and system tests so that the AV42 design would meet the design criteria of KTA 3501 (Reference 43), IEEE 279, IEEE 603, and Appendix B of 10 CFR Part 50.

5.1 AV42 PLD Logic Quality



The PLD design follows the traditional design path used for the design of safety-related equipment. Functional requirements were established with the use of design inputs, attributes and architecture. A design verification process ensured that the circuit was designed as planned. This proved that the original functional model (the design specification) satisfied the functional requirements that were established prior to the PLD design.

A verification and validation process was performed on the PLD design. This step was performed to remove any design errors before proceeding to the final manufacturing phase. Simulated sets of input patterns of the integrated AV42 circuit board were used to analyze the circuit variables. The test output patterns were required to conform to the projected output.

Finally, the manufacturing checking phase, which is the actual integrated test phase, verifies and validates the correctness of the manufacturing process of the PLD and the entire AV42 circuit board.



The testing requirements for the PLD design were all attained, documented, and established the completeness and correctness of the design. Competent, independent professionals witnessed, performed, and reviewed all necessary activities and tests. This independent survey of activities and tests provided high confidence that the PLD design was fault-free. The PLD design verification and validation process defined methods and procedures for ensuring the following:

- Earliest possible detection and elimination of design errors
- Enhancement of the quality and reliability of the AV42
- Improved transparency of project handling
- Minimization of the risk of the project overrunning costs and deadline
- Quick evaluation of future design changes to the PLD

The AV42 design documents including all revisions have been placed under a CM program that is discussed in Section 4.9. These documents are all reviewed, approved, and released in accordance with this CM program.

TUEV performed the independent third party review of the design, development, and testing process. After the manufacturing process was completed, TUEV completed the formal theoretical and functional testing and issued TUEV Report 968K 102.02/02 and TUEV Report 968K 102.05/03. This independent review verified that the safety requirements and stipulations defined in KTA 3503 (Reference 44) were met.

All components and modules of the TXS system including the AV42 have been designed and evaluated to be of a quality commensurate with the low failure rates required for safety systems. A robust PLD design and development methodology that emphasized early design assessment was used. The PLD is designed, manufactured, and tested using a process that meets the rigorous quality requirements of Appendix B of 10 CFR Part 50 and the guidance provided in ANSI/ASME NQA-1.



5.2 PROFIBUS® Controller



6.0 QUALIFICATION ANALYSIS

6.1 Environmental, Electrical, Seismic, EMC, ESD TESTING and Radiation Analysis

The environmental, electrical, seismic, and EMI and RFI testing initially were performed using the guidance of European standards. Additional testing that was performed followed the guidance and requirements of the NRC. The overall test program was conducted using AREVA NP program requirements which meet the requirements of Appendix B of 10 CFR Part 50. The requisite burn-in test, baseline functional test, and operability tests were performed successfully for additional testing. AREVA NP Summary Test Report 66-5065211-00 (Reference 49) provides the details for this additional testing.

6.2 Environmental

Environmental qualification was initially performed through type testing according to the process in German Safety Standards (KTA-3503) and technical requirements according to the applicable international IEC, IEEE, and DIN EN standards, as described below. Certificates and associated evaluation reports document the results of these type tests for the component type. Additionally, each qualified AV42 component passes a factory test that complies with the requirements of KTA 3507 (Reference 45) and has its own factory test certification by the responsible factory QA personnel. If a certified product requires modification, the modified product is required to have a new certification. Qualification was also required for the complete safety-related AV42 module.

DIN EN 60721-3-3 (Reference 39) governed the establishment of classifications for environmental conditions. The guidance of DIN EN 60068 Part 2-1 and Part 2-2 (Reference 42) was used for environmental testing procedures for both cold and dry heat. IEC 68 Part 2-3, Part 2-14 and Part 2-30 (Reference 35) provided guidance for the basic environmental testing procedures for damp heat-steady state, temperature change, and damp heat-cyclic, respectively.

The environmental tests that were performed for the AV42 module consisted of the following:

- Constant cold following rapid temperature change when not in operation

- -25°C (or -13°F) for 96 hours
- Constant heat following rapid temperature change when not in operation
 - 70°C (or 158°F) for 96 hours
- Constant damp heat when not in operation
 - 40°C (or 104°F) at 93 percent relative humidity for 96 hours
- Thermal cycling when not in operation
 - -25 — 70°C (or -13 — 158°F) for 3 hours at each temperature
- Cycled humidity when not in operation
 - Temperature and humidity per Figure 2a of IEC 68-2-30
- Constant damp heat during operation
 - 40°C (104°F) at 93 percent relative humidity for 24 hours
- Thermal cycling during operation
 - 0 — 55°C (or 32 — 131°F) for 3 hours; rate of change 3°C (5.4°F)/minute
- Cycled dry heat during operation, 1000 hours
 - 55°C (131°F) for 20 hours, 25°C (77°F) for 2 hours, 1 hour transition

The AV42 operated as required in the DIN and KTA standards environmental testing. TUEV Report 968K 102.02/02 provides additional details regarding the environmental testing. This testing provided the necessary confidence that this environmental profile does not degrade the AV42 components. The specified AV42 operating temperature range is 0 — 55°C (32 — 131°F). The climate class is 3K3 in accordance with DIN EN 60721-3-3.

The environmental testing to qualify the AV42 module to NRC standards was performed and completed in accordance with the guidelines of EPRI TR-107330. While the primary objective of EPRI TR-107330 is to provide generic requirements and guidance for qualifying commercial programmable logic controllers for use in nuclear safety-related applications, it also provides acceptable and proper guidance for qualifying most digital components, including the AV42. Therefore, its hardware qualification provisions were adopted for this qualification effort. Sections 4.3.6 and 6.3.3 of the EPRI report provide the environmental qualification details. AREVA NP Summary Test Report 66-5065211-00 provides a discussion of this testing, which

was designed to simulate the maximum temperature and humidity exposure conditions while performing its intended application and results. The test configurations for the baseline product replicated the typical installation at a U.S. nuclear plant with normal environmental temperature and humidity conditions and demonstrated that the AV42 module does not experience failures due to the range of conditions of temperature and humidity listed in EPRI TR-107330.

The temperature range for operability testing of the AV42 is ambient 4.4 to 60°C (40—140°F) over a relative humidity range of 5 to 90 percent. The temperature and humidity profile for the environmental stress testing duplicated the profile presented in EPRI TR-107330. The AV42 module operated as intended during and after exposure to the stress testing and met all performance requirements. Testing concluded that the AV42 module will not undergo any faults due to the temperature and humidity levels at the stress test conditions. The environmental testing was performed in accordance with EPRI TR-107330. AREVA NP Summary Test Report 66-5065211-00 provides the details for this testing.

The environmental testing proves that the AV42 complies with the requirements of GDC 4, 10 CFR 50.49 (Reference 2) and Section 5.4 of IEEE 603. The guidance presented in IEEE 323 (Reference 23) and the EPRI TR-107330 has been followed, and the results have been verified, which ensures that the AV42 design meets the functional performance requirements over the range of normal environmental conditions for the area in which it is to be located and will not experience failures due to abnormal service conditions of temperature and humidity.

6.3 Electrical

TUEV performed several electrical tests that focused on the direct current (DC) power supplies to determine the electrical characteristics of the AV42. The following tests were performed:

- Maximum current consumption
- Maximum power consumption
- Module insertion and removal
- Activation and deactivation:
 - Short term interruption

- Shutdown and startup
- Continuous voltage change
- Gradual power supply variations
 - Gradual deactivation
 - Gradual activation
 - Electrical isolation
 - Self-heating

During these tests, the power source variations were determined and tested to European guidance. The AV42 module electrical power supply functions were determined to be satisfactory. The testing determined the surge withstand capability requirements. Section 6.5 discusses this capability and the EMI and RFI testing in more detail.

Additional testing was performed on the AV42 power supply in accordance with EPRI and NRC guidance and regulations. The power supply hold-up test simulated a 40 milliseconds loss of input power to the power supplies. The Power supply output is to remain above 21 volts direct current (VDC) at both a 70 percent and 95 percent load. The testing was performed in accordance with the provisions outlined in EPRI TR-107330. The AV42 Power Supply output remained successfully at 24 VDC and was not interrupted. AREVA NP Summary Test Report 66-5065211-00 provides additional details for this test.

AREVA NP Summary Test Report 66-5065211-00 discusses the power supply testing in Section 3.7. AREVA NP Summary Test Report 66-5065211-00 Section 3.9 discusses the anomalies. AREVA NP Summary Test Report 66-5065211-00, Attachments 9—13, provide varied test data. A visual inspection of the AV42 was performed before any testing was performed. The AV42 module was required to operate as intended during and after the specified tests, and operate as intended after the testing. With plant specific installation, grounding and shielding for inputs and outputs to the AV42 are designed to meet the guidance provided in EPRI TR-102323 (Reference 32) and IEEE 1050 (Reference 29) as endorsed by Regulatory Guide 1.180 (Reference 17). The AV42 chassis and power supply attach an earth ground and DC common to grounding connection points. Shielding connections are provided with the I/O terminations and are optimized for noise protection. The power supply requirements of IEEE 603 are met.

6.4 Seismic

DIN EN 60721-3-3, DIN EN 60068 Part 2-6 and DIN EN 60068 Part 2-27 provide applicable European standards for seismic testing. AREVA NP Summary Test Report 66-5065211-00 provides the specifications and test results for seismic testing in accordance with the EPRI TR 107330, IEEE 344 (Reference 25), and Regulatory Guide 1.100 (Reference 15).

Seismic testing was part of the baseline qualification testing and was performed in accordance with the provisions of these standards. The AV42 module was required to operate as intended with all connections remaining intact and all modules fully inserted for the specified level of vibration. All functional parts and non-functional parts were required to meet their specified vibration levels. For the testing to the DIN standards, the AV42 was tested in five different seismic oriented tests:

- Operational vibrations
- Vibrations and seismic motion during operation
- Vibrations in the range of 5 – 100 Hz (aircraft crash)
- Transport stress
- Shock

TUEV Report 968K 102.02/02 discusses these test results in detail.

For the testing to the NRC guidance and requirements discussed in IEEE 344 and Sections 4.39 and 6.3.4 of EPRI TR-107330, a resonance search was conducted followed by five simulated Operating Basis Earthquakes (OBE) and one simulated Safe Shutdown Earthquake (SSE). Simulated vibrations were applied and operability tests were performed both before and after this seismic testing. Visual inspections were completed after the SSE test. Acceptable test results were reported for all seismic tests; however, the power supplies exceed the accuracy acceptance criteria by plus or minus 0.1 percent. This result was not deemed to be critical. AREVA NP Summary Test Report 66-5065211-00 discusses these results in more detail. The AV42 module met the performance requirements during and following the application of a SSE and five OBEs. The AV42 test module operated as intended during and after the application of the vibrations. During the testing, all connections remained intact and modules remained fully inserted. This

seismic testing ensures that the seismic qualification criteria for the AV42 module envelope those of U.S. nuclear plants and proves that the AV42 module is suitable for seismic qualification as a safety-related module. The AREVA NP seismic test report discusses seismic testing anomalies. Because of the weight of the equipment tested, the acceleration capability of the test table could not achieve 14 g. Previous seismic testing of other types of equipment has also recorded this variance. Successful operability testing was performed after the seismic testing. The AV42 seismic capability complies with the requirements of GDC 2 and Section 5.4 of IEEE 603 and the applicable guidance in the EPRI TR-107330, IEEE 344, and Regulatory Guide 1.100. This compliance demonstrates that the AV42 module is qualified as seismic Category 1 equipment.

6.5 EMC/ESD

EMI and RFI was part of the baseline type testing qualification using European standards. EMC was conducted in accordance with IEC 61000-6-2 (Reference 37), DIN EN 50081-2 (Reference 40), DIN EN 55011 (Reference 41), DIN EN 61000-4-2 (Reference 38), DIN EN 61000-4-3, DIN EN 61000-4-4, DIN EN 61000-4-5, DIN EN 61000-4-6, IEC 255-4 (Reference 36) and DIN EN 61000-4-2. There were eight distinct EMC tests performed by TUEV:

- Electro static discharge (ESD) immunity
6 Kilovolt (kV) contact discharge, 8 kV airborne discharge
- Electrical fast transient and burst immunity
Test voltage of 2 kV
- Conducted disturbances (radio frequency (RF) voltage)
15 Kilohertz (kHz)—80 Megahertz (MHz) at 10 Volt (V)
- Interference emission-radio interference radiation
30 MHz—230 MHz, 40 (decibel) dB and 230 MHz-1 Gigahertz (GHz), 47 dB
- Interference emission-radio interference voltage
9 KHz—30 MHz, 60 dB
- Electromagnetic field immunity
27 MHz—1 GHz, 10 volts/meter (V/m)

- Damped 1 MHz oscillatory magnetic field immunity
Signal lines-2 kV, Supply lines – 2 kV and 1 kV
- Conducted disturbances-surge voltage
Signal lines a-a 1 kV, a-PE 2 kV
Supply lines a-a .5 kV, a-PE 1 kV

During independent testing by TUEV, the AV42 demonstrated acceptable test results and compliance with immunity criteria. There were two issues identified during initial testing that required retesting, one of which required a change in protection to the module. However, both issues were resolved in supplementary testing. The test institute, TUEV, possesses European EMI and RFI testing records and appendices. TUEV Report 968K 102.02/02 contains summaries of the testing procedures and results.

The results of this testing indicated that the AV42 performed adequately and is fully qualified to European EMI and RFI levels. Radiated emissions testing was conducted in accordance with DIN EN 50081-2. EMC testing was performed in accordance with the guidance presented in IEC 61000 and DIN EN 55011. AREVA NP Document Number 01-1007841 (Reference 47) provides the specifications for the testing details for the EMI and RFI testing performed on the AV42 module.

Additional EMC testing was performed to demonstrate compliance with the guidance presented in EPRI TR-107330, EPRI-TR-102323, and Regulatory Guide 1.180. The susceptibility and emission testing to NRC regulations and industry standards is as follows:

Susceptibility Tests

1. MIL-STD 461E CS101 Conducted Susceptibility/Low Frequency, AC and DC Power Lines, 30 Hz to 150 KHz
2. MIL-STD 461E CS114 Conducted Susceptibility/High Frequency, AC and DC Power Lines and Signal Leads, 10 KHz to 200 MHz
3. MIL-STD 461E CS115 Conducted Susceptibility, Signal Leads for Two Amp Limit, Low and Medium Exposure Limit

4. MIL-STD 461E CS116 Conducted Susceptibility, Signal Leads, Damped Sinusoidal Transients, Signal Leads, 10 KHz to 100 MHz
5. MIL-STD 461E RS101 Radiated Susceptibility, System, Magnetic Field, 30 Hz to 100 KHz
6. MIL-STD 461E RS103 Radiated Susceptibility, System, Electric Field, 30 MHz to 10 GHz

Emission Tests

1. MIL-STD 461E CE101 Conducted Emissions/Low Frequency, DC Power Lines, 30 Hz to 10 KHz
2. MIL-STD 461E CE101 Conducted Emissions/Low Frequency, AC Power Lines < 1 KV, 60 Hz to 10 KHz
3. MIL-STD 461E CE101 Conducted Emissions/Low Frequency, AC Power Lines > 1 KV, 120 Hz to 10 KHz
4. MIL-STD 461E CE102 Conducted Emissions/High Frequency, 120 VAC Power Lines, 10 KHz to 10 MHz
5. MIL-STD 461E RE101 Radiated Emissions, Magnetic Field, Entire System, 30 Hz to 100 KHz
6. MIL-STD 461E RE102 Radiated Emissions, Electric Field, Entire System, 2 MHz to 10 GHz

IEC 61000 Tests

1. 61000-4-4 Fast Transient Impulse, +/- 2 KV and 4 KV Peak Pulse, Power Lines
2. 61000-4-5 Surge Immunity Combination Wave, Ring, Open and Short Circuit, Power Supply Lines
3. 61000-4-12, Surge Withstand Ring Wave, 100K HZ Wave, Power Lines
4. 61000-4-2, Electro Static Discharge, Accessible Test Points

EMI and RFI testing was performed in accordance with the guidance within the EPRI TR, applicable provisions of MIL-STD 461E (Reference 34), Regulatory Guide 1.180, and the applicable parts of IEC 61000. AREVA NP Summary Test Report 66-5065211-00 provides the EMI and RFI testing provisions and results. AREVA NP Summary Test Report 66-5065211-00

Section 3.8 discusses EMC. AREVA NP Summary Test Report 66-5065211-00 Section 3.9 discusses the anomalies. AREVA NP Summary Test Report 66-5065211-00, Attachments 9-13, provide varied test data. A visual inspection of the AV42 module was performed prior to any EMC testing. The AV42 was required to operate as intended during and after the specified EMC tests. There was one particular anomaly noted with the power supply in that the emission level was exceeded. After a new card for the power supply with a power factor correction was installed, the power supply passed the testing criteria. Another AV42 anomaly (i.e., fault flag not set) was attributed to cross-talk on the cables to the test machine. This was considered an isolated event. The EMI and RFI testing that was performed on the AV42 module provides a detailed definition of the characteristics and record of all applicable results.

The surge withstand testing demonstrated the suitability of the alternating current (AC) power line electrical surge withstand capability of the AV42. This testing shows that the AV42 module conforms to the applicable guidance of EPRI TR-107330, IEEE C62.41 (Reference 30), and IEEE C62.45 (Reference 31). In addition, the AV42 design met the requirements of IEC 61000 4-5 and 61000 4-12 that were used for test set up. For all test cases, the AV42 module operated continuously and conformed to all test criteria following the applications of the surge test voltages.

The electrical fast transient test was conducted on the power supply. This test conformed to the guidance specified in Regulatory Guide 1.180. The test specimen components operated as intended. The test specimen successfully passed IEC 61000-4-4 tests and was fully qualified by conforming to the levels in EPRI TR-102323 and Regulatory Guide 1.180.

The testing performed demonstrates the suitability of the equipment for enveloping all intended U.S. plant EMC environments. The results of the ESD testing conformed with the surge withstand capability guidance in EPRI TR-102323 and Section 4.6.2 of EPRI TR-107330. The AV42 design meets the requirements of GDC 4 and IEEE 603. Furthermore, the AV42 design conforms to the applicable guidance presented in Regulatory Guide 1.180, MIL-STD 461E, and IEC 61000. EPRI TR-102323 and TR-107330 were used to develop the appropriate criteria for testing the AV42 in this area.

6.6 Radiation

The AV42 equipment is designed to be located in a mild (i.e., non-harsh) environment. 10 CFR 50.49 defines a mild environment as "an environment that would at no time be significantly more severe than the environment that would occur during normal plant operation, including anticipated operational occurrences." Because of this, the environmental qualifications of the AV42 for a harsh environment are not included within the scope of the AV42 testing program.

The AV42 design meets the functional performance requirements for the radiation levels discussed above. The AV42 conforms to the guidance of the EPRI TR-107330, Regulatory Guide 1.89 (Reference 14), and IEEE 323. The AV42 also meets the requirements of GDC 4 and IEEE 603 for performance in a mild radiation environment.

7.0 RELIABILITY

7.1 Failure Modes and Effects Analysis

A system level Failure Modes and Effects Analysis (FMEA) will be performed for plant specific applications which use the AV42. Based on engineering judgment it is anticipated that the AV42 design does not result in any new failure modes that violate any design principle or regulation regarding failures and in particularly single and cascading failures. Given a postulated single failure of an AV42, the necessary plant safety functions will continue to be met through redundancy of plant systems. Due to functional isolation within the PLD, a single failure within the PROFIBUS[®] controller of the AV42 will not affect the safety functions of the AV42 module in accordance with the guidance of Regulatory Guide 1.53, (Reference 11) which endorses IEEE 379 (Reference 26).

The analysis shows that the chosen hardware, architecture, and implementation of the AV42 module sufficiently controls all postulated failure modes to prevent unallowable failures within the module. When installed in a plant specific redundant system, the failure of any AV42 component cannot prevent the system safety function from being correctly performed. The AV42 meets the requirements of IEEE 603 for this area.

7.2 Failure Rate Analysis

The AV42 reliability measurement is both a possible and desirable part of the reliability determination of a safety system. A failure rate, specifically, the number of failures per unit of time, is one measure of reliability. The measurement of AV42 reliability is similar to a measurement of safety system or hardware reliability and should be based on the same set of data (i.e., determine the number of failures per the amount of time in the test period).



7.3 Operating History

There are approximately 40 AV42 modules installed in the ATUCHA 1 Plant in Argentina that have been operating since March 2003. Also, there are approximately 600 Modules installed in TIANWAN 1 Plant in China that have been operating since August 2005. Operation to date at both sites has yielded no failures that affected the performance of the AV42. There is a formal process in place for TXS components such that anomaly reports will provide specific information including requirements or design inadequacies, qualitative data on failure modes, quantitative data on the AV42 module hardware and PLD logic reliability, and data on performance capability (e.g., capacity and throughput). As data is collected, it can be analyzed for MTBF in the integrated operational system by identifying problematic modules, failure detection and recovery effectiveness (i.e., coverage), and the rate of discovery of unanticipated hazards. This data provides an ongoing reliability calculation for the AV42 that allows failures and concerns to be easily identified and evaluated.

The quality of design and testability provided in the AV42 design is adequate to achieve a high functional reliability commensurate with the safety functions it performs. GDC 21 requires that the AV42 shall be designed for high functional reliability and in-service testability commensurate with the safety functions to be performed. The independence measures designed into the AV42 module and redundancy in plant components that the AV42 module actuates, when configured as a system, are sufficient to ensure that: (1) no single failure results in loss of the protection function and (2) removal from service of any component or channel does not result in loss of the required minimum redundancy. The AV42 permits the periodic testing of its functioning when the reactor is in operation including the capability to test channels independently to determine failures and losses of redundancy that may have occurred. The design of the AV42 meets the reliability and in-service testability requirements of both GDC 21 and IEEE 603.

8.0 CONCLUSIONS

The AV42 is designed and manufactured to very stringent criteria to meet all relevant nuclear standards. It is qualified for use in safety-related systems (e.g., ESFAS). The AV42 is qualified for environmental, seismic, and all EMI and RFI concerns. Qualification testing was performed in accordance with IEEE 323 and IEEE 344, Regulatory Guide 1.180, EPRI TR-102323, and EPRI TR-107330 guidance. For EMI and RFI testing, various DIN standards were followed along with the guidance from EPRI TR-107330, EPRI TR-102323, and Regulatory Guide 1.180. Suitability testing performed in Germany and the United States demonstrates that the design meets the requirements of GDC 2 and 4. NRC approval for this testing approach is requested.

The AV42 module is designed in accordance with the requirements of IEEE 603. Therefore, the design meets the requirements of 10 CFR 50.55a(h) for both module design issues and the qualification criteria for devices. The implementation of the AV42 design meets the functional requirements of safety-related systems, including ESFAS. The module does not affect the functional diversity of the safety systems and, in fact, enhances operator and system performance capabilities. The priority capabilities of the AV42 module will be set to ensure that all regulations and plant operational needs will be met. The automatic safety-related actuation capabilities will always be given priority over the non-safety-related actuation capabilities. Manual safety-related actuation capabilities are in accordance with IEEE 603 and Regulatory Guide 1.62 and will be given priority over both automatic and manual non-safety-related actuation capabilities.

The PLD development process meets the provisions of Appendix B of 10 CFR Part 50. The special characteristics associated with safety-related priority logic have been addressed. The design, manufacturing, and testing conducted on the PLD ensures that the PLD is not a credible source of common mode failure resulting from design errors or faults. The response time of the AV42 module is within the desired design limits so that plant response time requirements will continue to be met with the use of the AV42 module. Because the safety functional path consists of only logic gates, the design of the PLD ensures that gradual response time degradation is not credible. A catastrophic failure is the only failure type that could affect response time; however, other types of surveillances readily detect catastrophic failures. For example, plant specific

functional testing or calibrations are sufficient to determine the proper functionality and acceptable operability, including acceptable response time, for the AV42. NRC approval is requested for this approach of verifying response time of the AV42 module.

The calculated reliability of the AV42 module is sufficiently high so that the requirements of GDC 21 are met. When installed in a redundant system, a system level FMEA which includes the AV42 module should not reveal any failure concerns that fall outside the bounds of acceptability.

Through a combination of both at power and offline testing, the AV42 is fully testable and is operable with onsite and offsite electrical power, assuming only one source is available. The design of the AV42 meets the guidelines GDC 22 and the separation and independence guidelines of Regulatory Guide 1.75.

Because of the convergence of the safety and non-safety-related function and data, the independence of this interface is a particularly important area. Both the electrical and data interfaces are protected so that the design satisfies the control and protection interactions requirements of IEEE 603. For connections to non-safety systems, electrical isolation is provided by either the fiber optic connection to TXP control systems or use of a qualified isolation device for hardwired inputs from other non-safety systems. Failures of the non-safety systems or the non-safety PROFIBUS[®] controller on the AV42 are functionally isolated within the PLD from preventing a safety function from being performed as long as actuation priority is implemented correctly and in accordance with plant specific requirements. The separation, reliability and independence requirements of GDC 24 are met.

This report demonstrates AV42 compliance to Class 1E equipment design, qualification, and quality criteria as well as criteria for the prioritization of safety-related signals and for the electrical separation and independence of redundant systems. NRC approval of the AV42 as a fully qualified safety-related actuation device is requested.

The AV42 module can be used in both the ESFAS and the ATWS system while maintaining the requirements of 10 CFR 50.62. For this application, the AV42 ensures system based

prioritization as required and configured on an application specific basis. NRC approval of the AV42 in both the ESFAS and ATWS system as a final actuation component is requested.

In conclusion, the AV42 module provides the hardware design solution and licensing bases for the signal interface between sense and command inputs from safety-related Class 1E main control board actuators, safety-related Class 1E TXS instrumentation and control system outputs, and non-safety-related Class 1E control actuations (including both automation (TXP AP) and manual (OM690)), and the execute feature for actuation and driver devices (including checkback signals) to the safety-related actuation devices using the AV42 module. The AV42 successfully monitors and controls safety-related actuators and drivers. The AV42 prioritizes the various sense and command inputs and executes an output that reflects the plant licensing and operational preferences. In addition, it monitors the checkback signals from the actuators and drivers and takes the appropriate action. The AV42 can process commands from all areas (e.g., inputs received from safety and non-safety-related instrumentation and control systems, automatic and manual portions of systems, and main control room and remote shutdown station). The AV42 module supports the design of highly integrated control room that provide operators with the capability to control safety-related motors and actuators from multiple sources (e.g., main control room screen-based soft controls). The AV42 provides this capability while meeting the licensing provisions for ESFAS as discussed in NUREG-0800.

9.0 REFERENCES

U.S. Regulations

1. 10 CFR 50.48, "Fire Protection."
2. 10 CFR 50.49, "Environmental Qualification of Electric Equipment Important to Safety for Nuclear Power Plants."
3. 10 CFR 50.55a, "Codes and Standards."
4. 10 CFR 50.55a(h), "Protection and Safety Systems."
5. 10 CFR 50.62, "Requirements for Reduction of Risk from Anticipated Transients Without Scram (ATWS) for Light-Water-Cooled Nuclear Power Plants."
6. 10 CFR Part 50 Appendix A, "General Design Criteria for Nuclear Power Plants."
7. 10 CFR Part 50, Appendix B, "Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants."
8. 10 CFR Part 50, Appendix R, "Fire Protection Program for Nuclear Power Facilities Operating Prior to January 1, 1979."

U.S. Regulatory Guidance

9. NRC Regulatory Guide 1.22, "Periodic Testing of Protection System Actuation Functions" dated February 1972
10. NRC Regulatory Guide 1.47, "Bypassed and Inoperable Status Indication for Nuclear Power Plant Systems" dated May 1973.
11. NRC Regulatory Guide 1.53, Revision 2, "Application of the Single-Failure Criterion to Nuclear Power Plant Protection Systems."

12. NRC Regulatory Guide 1.62, "Manual Initiation of Protective Actions" dated October 1973
13. NRC Regulatory Guide 1.75, Revision 3, "Physical Independence of Electrical Systems."
14. NRC Regulatory Guide 1.89, Revision 1, "Environmental Qualification of Certain Electric Equipment Important to Safety for Nuclear Power Plants."
15. NRC Regulatory Guide 1.100, Revision 2, "Seismic Qualification of Electric and Mechanical Equipment for Nuclear Power Plants."
16. NRC Regulatory Guide 1.118, Revision 3, "Periodic Testing of Electrical Power and Protection Systems."
17. NRC Regulatory Guide 1.180, Revision 1, "Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems."
18. NUREG-0800, "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants," (Chapter 7) Revision 4, June 1997.
19. NUREG-0800, "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants," BTP-HICB-11, "Guidance and Qualification of Isolation Devices," Revision 4, June 1997.
20. NUREG-0800, "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants," BTP-HICB-19, "Guidance on Evaluation of Defense-in-Depth in Digital Computer-Based Instrumentation and Control Systems", Revision 4, June 1997.

U.S. Industry Standards

21. ANSI/ASME NQA-1-1994, "Quality Assurance Requirements for Nuclear Facility Applications."
22. IEEE Standard 279-1971, "Criteria for Protection Systems for Nuclear Power Generating Stations."
23. IEEE Standard 323-2003, "Qualifying Class 1E Equipment for Nuclear Power Generating Stations."
24. IEEE Standard 338-1987, "Criteria for the Periodic Surveillance Testing of Nuclear Power Generating Station Safety Systems."
25. IEEE Standard 344-1987, "Seismic Qualification of Class 1E Electric Equipment for Nuclear Power Generating Station."
26. IEEE Standard 379-2000, "Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems."
27. IEEE Standard 384-1992, "Criteria for Independence of Class 1E Equipment and Circuits."
28. IEEE Standard 603-1991, "Criteria for Safety Systems for Nuclear Power Generating Stations."
29. IEEE Standard 1050-1996, "Guide for Instrumentation and Control Equipment Grounding in Generating Stations."
30. IEEE Standard C62.41-1991, "Recommended Practice on Surge Voltages in Low-Voltage AC Power Circuits."
31. IEEE Standard C62.45-1992, "Guide on Surge Testing for Equipment Connected to Low-Voltage AC Power Circuits."

32. EPRI-TR-102323, Revision 2, "Guidelines for Electromagnetic Interference Testing for Power Plant Equipment," 2000.
33. EPRI-TR-107330, "Generic Requirements Specification for Qualifying a Commercially Available PLC for Safety-Related Applications in Nuclear Power Plants," 1996.
34. MIL-STD 461E, "Requirements for the Control of Electromagnetic Interference Characteristics of Subsystems and Equipment," U. S. Department of Defense, August 20, 1993.

International Standards

35. IEC 68-1986/1987, "Environmental Testing."
36. IEC 255-1976, "Electrical Relays."
37. IEC 61000, "Electromagnetic Compatibility," 1995-2000 (Part Dependence).
38. IEC 61000-4, "Electromagnetic Compatibility - Part 4: Testing and Measurement Techniques."
39. DIN EN 60721-3-3-1995, "Climatic Environmental Conditions."
40. DIN EN 50081-2, "Electromagnetic Compatibility – Generic Emission Standard Part 2: Industrial Environment."
41. DIN EN 55011, "Industrial, Scientific, and Medical (ISM) Radio-Frequency Equipment," 1997.
42. DIN EN 60068-1994/1995, "Environmental Testing."
43. KTA 3501-1985, "Reactor Protection Systems and Monitoring Devices of the Safety System."
44. KTA 3503-1986, "Type Test of Electrical Modules for the Reactor Protection System."

-
45. KTA 3507-1997, "Factory Test."

Regulatory Review Precedent

46. Letter dated May 5, 2000, from Stuart A. Richards, NRC, to Jim Mallay, Siemens Power Corporation, 'Acceptance for Referencing of Licensing Topical Report EMF-2110 (NP), Revision 1, "TELEPERM XS: A Digital Reactor Protection System" (TAC NO. MA1983).'

AREVA NP Documents

47. AREVA NP Document 01-1007841-00, "TELEPERM XS AV42 Priority Module-Data Sheet," January 6, 2002.
48. AREVA NP Document 51-5052273-00, "TXS Radiation Qualification."
49. AREVA NP Summary Test Report 66-5065211-00, "Surveillance and Functional Test Report for Additional Equipment," dated December 14, 2005.
50. Siemens Topical Report EMF-2110, Revision 1, "TELEPERM XS: A Digital Reactor Protection System," September 1, 1999.
51. TELEPERM XP, Software Description for the AS620 Automation System, Field Device Function Block FB146 AV42_ESG22, Siemens 2001.
52. TUEV Report 968K 102.02/02, "Documentation of theoretical and practical testing in accordance with KTA 3503 of priority module AV42 in the TELEPERM XS system From AREVA NP GmbH," June 26, 2002.
53. TUEV Report 968K 102.05/03, "Comments on the Amendments to Priority Module AV42 of the TELEPERM XS System of AREVA NP GmbH," December 9, 2003.