Enclosure 2

Defense in-Depth and Diversity Assessment

(Non-Proprietary)

0 ABSTRACT

AmerenUE and Wolf Creek Nuclear Operating Corporation (WCNOC) are planning to replace existing safety and non-safety related instrumentation and control systems with digital systems in their respective licensed facilities. AmerenUE and WCNOC are replacing the analog Reactor Trip System (RTS) and the Nuclear Steam Supply Engineered Safety Features Actuation System (NSSS ESFAS) with a digital computer-based Reactor Protection System (RPS), the Framatome Advanced Nuclear Power (FANP) TELEPERM XS (TXS). In addition, the Nuclear Instrumentation System (NIS), Load Shedder and Emergency Load Sequencer (LSELS), the Balance of Plant Engineered Safety Features Actuation System (BOP ESFAS), Main Steam and Feedwater Isolation System (MSFIS), the Emergency Diesel Generator (EDG) Control System, the Thermocouple Core Cooling Monitor (TC/CCM), Reactor Vessel Level Indicating System (RVLIS) and the Class 1E Analog Controls are being replaced with the TXS system. Furthermore, TXS will provide data to a Class 1E Qualified Display System. The Qualified Display System consists of flat screens that provide the operator with Post Accident Monitoring System and selected Regulatory Guide 1.97 safety related variables in a screen-based main control room environment. As part of the overall Instrumentation and Control (I&C) upgrade, the non-Class 1E I&C systems and the plant computer will also be upgraded using the Siemens process control system, TELEPERM XP (TXP), and its operation and monitoring system, OM690.

Overall, the planned I&C modernization will enhance the operation of the Callaway Plant and Wolf Creek Generating Station (WCGS) and at the same time improve the safety and emergency response capability over the long term operation of the plant. The digital systems chosen to replace existing safety and non-safety related I&C systems have improved surveillance and diagnostic features, high integrity fault tolerant architectures, and fail-safe behavior. The overall upgrade plan is to install selected systems over the course of several refueling outages. It can be demonstrated that the overall upgrade can be installed systematically in any sequence without any adverse affects on the affected systems' response capabilities.

The installation of a digital-based computerized system that includes the Reactor Trip functions and the ESFAS functions, however, presents a safety and licensing concern that a postulated common-mode failure of the digital-based components might propagate in such a fashion to defeat safety functions in redundant safety related channels. This would in effect preclude the initiation of required safety functions assumed in FSAR/USAR Chapter 15 analyses. This report demonstrates that FANP, AmerenUE, and WCNOC have adequately addressed the ability of the proposed digital I&C systems to withstand the vulnerabilities of postulated common-mode failures by providing inherent defense-in-depth and diversity (D-in-D&D).

The Nuclear Regulatory Commission (NRC) has established a methodology and acceptance criteria for D-in-D&D evaluations that are to be used when digital-based systems are implemented in operating nuclear power plants. This methodology and acceptance criteria are documented in the NUREG 0800, "Standard Review Plan for the Review of Safety Analysis

Reports for Nuclear Power Plants," Branch Technical Position (BTP) HICB-19, "Guidance for Evaluation of Defense-in-Depth and Diversity in Digital Computer-Based Instrumentation and Control Systems."

Pursuant to the guidance of BTP HICB-19, the capability of the Callaway Plant and WCGS digital upgrade design to withstand a hypothetical software common-mode failure affecting RTS, NSSS ESFAS and BOP ESFAS functions is assessed in this report. Based on the D-in-D&D built into the TXS design, the assessment considers failures attributable to common-mode failures and qualitatively reanalyzes the system response to each of the applicable FSAR/USAR Chapter 15 accidents as well as additional selected transients and accidents (such as Containment Functional Design, High Energy Line Break, and Main Steam Line Break outside containment). The evaluation is thus performed to determine if the concepts for D-in-D&D adequately address concerns about software common-mode failure using the NRC guidance and acceptance criteria of BTP HICB-19.

This report concludes that FANP, AmerenUE, and WCNOC can demonstrate that the different TXS applications have sufficient design D-in-D&D to cope with postulated software common-mode failures. The qualitative re-evaluation of FSAR/USAR analyzed events confirms that sufficient D-in-D&D exists in the design of the proposed I&C digital upgrade to meet the criteria established by the NRC's guidance in BTP HICB-19. This is based, in part, on the determination that due to the D-in-D&D design of the TXS, the worst-case common-mode failure is not system-wide, i.e., one that could completely disable the RTS and/or ESFAS. The report thus concludes that the selection and design of TXS hardware and software components prevents the Callaway Plant and WCGS TXS applications from being susceptible to a software common-mode failure that disables any safety function. The methods selected for the TXS design provide for a new system that will effectively replace existing systems without adding any new or complex systems to the plant.

It is also concluded in this report that the D-in-D&D concepts utilized in the design of the planned upgrades continue to meet the Anticipated Transient Without Scram (ATWS) rule and that enhanced diverse control and monitoring features are provided using the TXP system. Displays and manual controls for safety critical functions initiated by operator action are independent and diverse from the TXS software used to perform the automatic portions of RTS, NSSS ESFAS, and BOP ESFAS, resulting in a design more typical of Advanced Light Water Reactor D-in-D&D designs. It may further be noted that, with respect to the TXS design, at least two independent echelons of defense are provided for each postulated event to protect against postulated, yet implausible, software common-mode failure. If a software common-mode failure were to occur, all automatic safety functions and manual system-level actuations would be available to mitigate postulated events. Due to the TXS system's diverse design features, a postulated software common-mode failure is limited to the extent that the RTS and the ESFAS remain available during such an occurrence, albeit with only half-channel capacity.

RECORD OF REVISION

Revision	Changed Sections	Description/Change Authorization
Rev. 0	All	Initial Issue of Document
Rev.1	All	Issue incorporating Callaway and Wolf Creek review comments. Incorporated Callaway Licensing and Safety analysis review comments and minor editorial comments

TABLE OF CONTENTS

LIST OF FIGURES

1 INTRODUCTION

AmerenUE and Wolf Creek Nuclear Operating Corporation (WCNOC) are replacing the analog Reactor Trip System (RTS) and the Nuclear Steam Supply Engineered Safety Features Actuation System (NSSS ESFAS) with a digital computer-based Reactor Protection System (RPS), the Framatome Advanced Nuclear Power (FANP) TELEPERM XS (TXS). In addition, the Nuclear Instrumentation System (NIS), Load Shedder and Emergency Load Sequencer (LSELS), the Balance of Plant Engineered Safety Features Actuation System (BOP ESFAS), Main Steam and Feedwater Isolation System (MSFIS), the Emergency Diesel Generator (EDG) Control System (Callaway only), the Thermocouple Core Cooling Monitor (TC/CCM), Reactor Vessel Level Indicating System (RVLIS) and the Class 1E Analog Controls are being replaced with the TXS system. Furthermore, the TXS system will provide data to a Class 1E Qualified Display System. The Qualified Display System consists of flat screens that provide the operator with Post Accident Monitoring System and selected Regulatory Guide 1.97 safety related variables in a screen-based main control room environment. Included in the overall Instrumentation and Control (I&C) upgrade, the non-Class 1E I&C systems and the plant computer will also be upgraded using the Siemens process control system, TELEPERM XP (TXP), and its operation and monitoring system, OM690.

Overall, the planned I&C modernization will enhance the operation of the Callaway Plant and Wolf Creek Generating Station (WCGS) and at the same time improve the safety and emergency response capability over the long term operation of the plant. The digital systems chosen to replace existing safety and non-safety related I&C systems have improved surveillance and diagnostic features, high integrity fault tolerant architectures, and fail-safe behavior. The overall upgrade plan is to install selected systems over the course of several refueling outages. It can be demonstrated that the overall upgrade can be installed systematically in any sequence without any adverse affects on the affected systems' response capabilities.

The installation of a digital-based computerized system that includes the RTS functions and the ESFAS functions, however, presents a safety and licensing concern that a postulated single software common-mode failure of the digital based components might propagate in such a fashion to defeat safety functions in redundant safety related channels. This could in effect preclude initiating required safety function actions assumed in FSAR/USAR Chapter 15 analyses. This report demonstrates that FANP, AmerenUE, and WCNOC have adequately addressed the ability of the proposed digital I&C systems to withstand the vulnerabilities of postulated common-mode failures by providing inherent D-in-D&D. Hardware failures associated with environmental, seismic, and electromagnetic interference/radio frequency interference (EMI/RFI) were previously addressed in Topical Report EMF-2110(NP), Reference /2/ and the TXS safety evaluation, Reference /29/.

The purpose of the overall assessment is to demonstrate that FANP, AmerenUE, and WCNOC have adequately addressed D-in-D&D and the ability of the proposed digital I&C systems to withstand vulnerability to postulated common-mode failures that could occur based on the design of the TXS hardware and software. The method described in EMF-2267 (P), "Siemens

Power Corporation Methodology Report for Diversity and Defense-in-Depth," (Reference /6/) was used as guidance for preparing this assessment and satisfying NRC guidance and acceptance criteria. FANP applied the generic methodology of FANP Topical Report EMF-2267 in a limited fashion to FANP Topical Report EMF-2340 (Reference /7/). This generic concept received NRC approval in Reference /29/.

The D-in-D&D assessment provided in this report evaluates replacing the analog RTS and ESFAS instrumentation with a digital computer-based TXS system. The report also considers how other safety and non-safety related system replacements proposed in the overall I&C digital upgrade impact or enhance D-in-D&D.

The TXS system for plant protection system applications will use simple hardware and software design architecture and features to prevent the occurrence of software common failure modes and effects. Special emphasis is given to the diversity of RTS and ESFAS safety related functions and the prevention of software failures. This report examines these failure mode and effect preventative techniques as they apply to system vulnerability to common-mode failures. These design architecture and features are extended to other TXS applications to achieve high levels of confidence in all areas: quality, integrity, diversity, fault tolerance, dependability, reliability, and availability. Diverse design architecture and features used in the TXS system include but are not limited to:
[

]

6. TXS Voters and Master/Checker CPUs: Voting of actuation signals will now use inputs from all protections sets. Checking by master/checker voter pairs of CPUs provide an additional level of redundancy.
7. On-line signal validation: Signal validation is used to eliminate questionable or faulted input data.
8. Watchdog Monitoring: Independent watchdog circuitry ensures outputs de-energize to predefined states when the CPU exceeds acceptable application program or self-monitoring program cycle times, or is initiated due to special exception handling.
9. Independent Indication, Monitoring, and Manual Controls: Hardware is selected that provides indication, monitoring, and manual controls independent of TXS software.
10. Diverse Plant Information and Controls Systems: Provisions are made to provide signals to Plant I&C Systems and ATWS Mitigation System Actuation Circuitry (AMSAC)

that are independent of the TXS software. Functions for these systems are performed by systems diverse from TXS, e.g., TXP.

For the assessment described in this report, each of the above design features was carefully considered and applied to the RTS and ESFAS, as well as other TXS applications, with regard to their capability to handle all postulated software common failure modes and effects. Considering the TXS design, system blocks were further analyzed for software common-mode failure vulnerability to determine the worst-case common-mode failure(s) for the TXS applications. Consideration was then given to each of the accidents and transients evaluated in the FSAR/USAR such that each event was qualitatively re-evaluated when assumed to occur in conjunction with the worst-case, common-mode failure, pursuant to the NRC guidance of NUREG 0800, "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants," Branch Technical Position (BTP) HICB-19 "Guidance of Evaluation of Defense-in-Depth and Diversity in Digital Computer-Based Instrumentation and Control Systems" (Reference /1/). The acceptable results of this evaluation, applicable to both Callaway Plant and WCGS, are summarized in the report.

Each section of the report, following this Introduction section (i.e., Section 1), is briefly introduced / summarized as follows:

Section 2 of this report discusses the regulatory position as described in BTP HICB-19, and NUREG/CR-6303, "Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems" (Reference /10/). In addition, the regulatory bases and other applicable guidance are cited followed up with a discussion of the acceptance criteria to be used for the D-in-D&D assessment.

Section 3 of this report presents the assessment methodology used by FANP, AmerenUE, and WCNOC to address the NRC's position for coping with a common-mode failure to the RTS and ESFAS. The NRC staff has established a methodology and provided acceptance criteria for D-in-D&D assessments for implementing digital computer-based systems in operating nuclear power plants. The methodology and acceptance criteria are documented in BTP HICB-19. Pursuant to this methodology, Section 3 describes the four echelons of defense, partitioning the system into blocks/modules, forms of diversity assessed, failure types, and assumptions. The realistic assumption conditions, operator actions, and the FSAR/USAR event-specific evaluation process are described. It concludes with identifying the goals of the assessment and a summary of the individual tasks used to perform the assessment.

Section 4 describes the I&C digital system upgrade. The system selected for the digital safety I&C system is TXS, as described in Topical Report EMF-2110 (NP), Revision 1 (Reference /2/). This section provides details about the major blocks of the digital I&C upgrade pertaining to echelons of defense. Systems associated with the RPS, RTS, ESFAS and ESFAS Support Systems, Monitoring and Indication Systems, and pertinent portions of the TXP control systems are discussed as well as discussions about Safe Shutdown Instrumentation, the Qualified Display System, AV42 Priority Control Modules (AV42), Monitoring and Service Interfaces, and the Gateway. The section provides the design basis as described in the FSAR/USAR (References /5/ and /24/) and identifies the safety functions that will be performed by TXS systems.

Section 5 examines the basic individual building block of the overall I&C upgrade, the TXS system design itself. The TXS system architecture and each of the design architecture and features techniques used to prevent hardware and software failures are discussed in detail. Sub-blocks within the TXS system design are identified and used to assess TXS system vulnerability to common-mode failures. The section describes identical as well as non-identical features of the system hardware and software. The diversity between TXS RTS and ESFAS applications and other TXS applications are discussed followed by further discussions about implementation of the overall digital I&C upgrade. The section then provides conclusions about the TXS system's vulnerability to common-mode failures and the ability to implement the overall digital upgrade while maintaining sufficient D-in-D&D.

Section 6 examines aspects of high integrity design that contribute to TXS system dependability: aspects pertaining to quality, design, reliability, availability, and configuration control. The design attributes of the TXS system that add positive attributes to TXS quality are discussed along with a discussion about TXS's deterministic features. Other aspects discussed are the quality of the system hardware and software design process, aging, operational considerations, availability, software quality assurance, testing, testability, and hardware/software configuration control. Section 6 also discusses quality as it relates to the diverse non-safety related TXP system.

Section 7 presents the systems that are diverse from TXS presented in Section 5. These systems are selected from the four echelons of defense as discussed in Section 3. The systems discussed in this section are diverse systems that would be available to provide a defense-in-depth capability assuming a total failure of the TXS RTS and ESFAS. The diversity between the TXP and TXS systems is discussed. Diverse AMSAC and diverse manual system and component actuation capabilities are described along with diverse indications that remain available. These diverse systems and manual actions/indications provide the defense-in-depth capabilities for the Callaway Plant and WCGS design that enable it to terminate and or mitigate most analyzed events in the unlikely event that the RTS and/or ESFAS fail to operate.

Section 8 summarizes the results obtained from qualitative assessment of the TXS design with respect to its capability to respond to each of the accidents and transients that are analyzed in the FSAR/USAR, assuming the worst-case common-mode failure described in Sections 4 and 5 of the report. This assessment is performed for the RTS and ESFAS, while not taking credit for any safety or non-safety related system that is subject to the same software common-mode failure. The conclusion of this section addresses compliance with acceptance criteria and summarizes that both safety and non-safety related methods are provided for all transients and accidents in the Callaway Plant FSAR licensing basis (Reference /5/) and the WCGS USAR licensing basis (Reference /24/).

Section 9, the conclusion, provides the FANP, AmerenUE, and WCNOC perspective on the results of the assessment.

1.1 REFERENCES

/1/ NUREG-0800, "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants," Branch Technical Position HICB-19, "Guidance for Evaluation of Defense-in-Depth and Diversity in Digital Computer-Based Instrumentation and Control Systems," Revision 4, June, 1997.

/2/ Siemens Topical Report EMF-2110, Revision 1, "TELEPERM XS: A Digital Reactor Protection System," September 1, 1999; FANP ID No.: 38-1288541-00.

/3/ EPRI Technical Report (TR)-102348, Revision 1, "Guidelines on Licensing Digital Upgrades," March 2002.

/4/ NRC Regulatory Issue Summary 2002-22, "Use of EPRI/NEI Joint Task Force Report, "Guideline on Licensing Digital Upgrades: EPRI TR-102348, Revision 1, NEI01-01: A Revision of EPRI TR-102348 to Reflect Changes to the 10 CFR 50.59 Rule,"" November 25, 2002.

/5/ Callaway Nuclear Plant Final Safety Analysis Report, OL-13, May 2003.

/6/ Siemens Topical Report EMF-2267: "Siemens Power Corporation Methodology Report for Diversity and Defense-In-Depth," August 1999; FANP ID No.: 38-1288542-00.

/7/ Siemens Topical Report EMF-2340, Revision 0: "Siemens Power Corporation Diversity and Defense-In-Depth Assessment In Accordance With the Methodology of EMF-2267," January 2000; FANP ID No.: 38-1288543-00.

/8/ NUREG-0493, "A Defense-in-Depth & Diversity Assessment of the RESAR-414 Integrated Protection System," March 1979.

/9/ Code of Federal Regulations Title 10 Part 50, Revised as of January 1, 2002.

/10/ NUREG/CR-6303, "Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems," December 1994.

/11/ 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)."

/12/ IEC 880, "Software for Computers in the Safety Systems of Nuclear Power Stations," 1986.

/13/ IEC 880, Supplement 1 Draft, "Software for Computers in the Safety Systems of Nuclear Power Stations," 1996.

/14/ Regulatory Guide 1.152, Revision 1, "Criteria for Digital Computers in Safety Systems of Nuclear Power Plants," January 1996.

/15/ Code of Federal Regulations Title 10 Part 50.62, "Requirements for Reduction of Risk From Anticipated Transients Without Scram (ATWS) Events for Light-Cooled Nuclear Power Plants."

/16/ ANSI/IEEE Std 279-1971, "Criteria for Protection Systems for Nuclear Power Generating Stations."

/17/ ANSI/IEEE Std 379-1988, "Standard Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems."

/18/ IEEE Std 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations."

/19/ Regulatory Guide 1.153, Revision 1, "Criteria for Safety Systems," June 1996.

/20/ Regulatory Guide 1.53, "Application of the Single-Failure Criterion to Nuclear Power Plant Protection Systems," June 1973.

/21/ SECY 91-292, "Digital Computer Systems for Advanced Light-Water Reactors," September 1991.

/22/ SECY 93-087, "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs," April 2, 1993.

/23/ Staff Requirements Memorandum on SECY 93-087, "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs," July 15, 1993.

/24/ Wolf Creek Updated Safety Analysis Report, Revision 16, March 11, 2003.

/25/ Burnett, T. W. T., et. al., "Westinghouse Anticipated Transients Without Trip Analysis," WCAP-8330, Non-Proprietary, Westinghouse Electric Corporation, August 1974.

/26/ Letter, NS-TMA-2182, Anderson, T. M. (Westinghouse Electric Corporation) to Hanaur, S. H. (USNRC), "ATWS Submittal", Non-Proprietary, December 30, 1979.

/27/ Ameren/UE Callaway FSAR Change Notice, "Revises the FSAR to Incorporate the Changes Made ... to the Containment Equipment Hatch. ...," CN Number 01-030, October 11, 2002.

/28/ Regulatory Guide 1.97, Revision 3, "Instrumentation for Light-Water-Cooled Nuclear Power Plants to Assess Plant and Environs Conditions During and Following an Accident," May 1983.

/29/ Safety Evaluation by the Office of Nuclear Reactor Regulation, Siemens Power Corporation Topical Report EMF-2110(NP), "TELEPERM XS: A Digital Reactor Protection System, Project No. 702.

/30/ Field Failure Rate calculation and Statistics of TELEPERM XS, Status 2003-06-30; FANP GmbH Document ID: FANP NGLTH/02/056.

/31/ Summary Test Report (STR), "TXS Supplemental EQ Summary Test Report"; FANP ID: 66-5015893-00.

1.2 DEFINITIONS

Administrative Controls - Rules, orders, instructions, procedures, policies, practices, and designations of authority and responsibility.

Anticipated Operational Occurrence - Those conditions of normal operation which are expected to occur one or more times during the life of the nuclear power unit and include, but are not limited to, loss of power to all recirculation pumps, tripping of the turbine generator set, isolation of the main condenser, and loss of all off-site power.

Block – Smallest portion of the system under analysis for which it can be credibly assumed that internal failures, including the effects of software errors will not propagate to other equipment.

Channel Set - An arrangement of components and modules as required to generate a single protective action signal when required by a generating station condition. A channel loses its identity where single protective action signals are combined.

Class 1E - The safety classification of the electric equipment and systems that are essential to emergency reactor shutdown, containment isolation, reactor core cooling, and containment and reactor heat removal, or are otherwise essential in preventing significant release of radioactive material to the environment.

Common-Cause Failure - Failure, which is the result of one or more events, causing coincident failures of two or more separate channels in a multiple channel system, leading to system(s) failure.

Common-Mode Failure - Multiple failures of systems, structures, or components as a result of a single phenomenon such as human error, fire or degradation of the properties of materials or hardware (even at different locations).

Design Basis Accident - A limiting plant process condition postulated and analyzed to conduct the site evaluation required by 10 CFR 100, "Reactor Site Criteria."

Design Basis Event - Postulated event used in the design to establish the acceptable performance requirements for the structures, systems, and components.

Diverse instrumentation and control systems (diverse I&C) – Per NUREG-0800, those systems provided expressly for diverse backup of the reactor trip system and engineered safety features actuation systems. Diverse I&C systems account for the possibility of common-mode failures in the protection systems. Diverse I&C systems include the anticipated transient without scram (ATWS) mitigation system as required by 10 CFR 50.62. For plants with digital computer-based instrumentation and controls, diverse I&C systems may also include hardwired manual controls, diverse displays, and any other systems specifically installed to meet the guidance of the Staff

Requirements Memorandum on SECY-93-087, "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs."

Diversity - A principle in implementation systems of sensing different parameters, using different technologies, using different logic or algorithms, or using different actuation means to provide several ways of detecting and responding to a significant event. Diversity is complementary to defense-in-depth and increases the chances that defenses at a particular level or depth will be actuated when needed. Defenses at different levels of depth may also be diverse from each other. (NUREG/CR-6303).

Division - The designation applied to a given system or set of components that enables the establishment and maintenance of physical, electrical, and functional independence from other redundant sets of components. (Also referred to as a Protection Set)

Hot Shutdown - The condition, in which the reactor is subcritical, and the reactor and its cooling system are at or near power operating temperatures.

Independence – Each channel (and each train) is physically and electrically independent. This ensures a single failure will affect only one of the redundant channels (or trains).

Redundancy – The parameters used have redundant channels. Sufficient redundancy will allow a coincident logic scheme such that a spurious signal will neither cause nor prevent a trip and/or safeguards actuation. Also, two trains of coincident logic are provided either being capable of initiating the required actuation.

Safety Function - One of the processes or conditions (for example, emergency negative reactivity insertion, post-accident heat removal, emergency core cooling, post-accident radioactivity removal, and containment isolation) essential to maintain plant parameters within acceptable limits established for a design basis event.

Safety System - A system that is relied upon to remain functional during and following design basis events to ensure: (1) the integrity of the reactor coolant pressure boundary, (2) the capability to shut down the reactor and maintain it in a safe shutdown condition, or (3) the capability to prevent or mitigate the consequences of accidents that could result in potential off-site exposures comparable to the 10 CFR Part 100 guidelines.

1.3 ABBREVIATIONS

A	Ampere
A/D	Analog to Digital
AC	Alternating Current
AFAS	Auxiliary Feedwater Actuation Signal
AFW	Auxiliary Feedwater
AMSAC	ATWS Mitigation System Actuation Circuitry
ANS	American Nuclear Standard
AP	Application Processor
ASIC	Application Specific Integrated Circuit
ASP	Auxiliary Shutdown Panel
ATWS	Anticipated Transients Without Scram
AUX	Auxiliary
AV42	Priority Control Module
BiCMOS	Bimetallic Complimentary Metal Oxide Semiconductor
BOP	Balance of Plant
BKR	Breaker
BTP	Branch Technical Position
BWR	Boiling Water Reactor
CET	Core Exit Thermocouples
CFR	Code of Federal Regulations
CMF	Common-Mode Failure
CPGA	Ceramic Pin Grid Array
CPIS	Containment Purge Isolation Signal
CPU	Central Processing Unit
CR	Control Room
CRC	Cyclic redundancy check (method for creating checksums)
CRDM	Control Rod Drive Mechanism
CRVIS	Control Room Ventilation Isolation Signal
CST	Condensate Storage Tank

CVCS	Chemical and Volume Control System
DBA	Design Basis Accidents
DBE	Design Basis Events
DCS	Distributed Control System
DG	Diesel Generator
D-in-D&D	Defense-in-Depth and Diversity
DNBR	Departure from Nucleate Boiling Ratio
DSS	Diverse Scram System
ECC	Emergency Core Cooling
ECCS	Emergency Core Cooling System
EDG	Emergency Diesel Generator
EEPROM	Electrical Erasable Programmable Read Only Memory
EMI	Electromagnetic Interference
EOP/EMG	Emergency Operating Procedure
ERG	Emergency Response Guideline
ES	Engineering Station
ESF	Engineered Safety Feature
ESFAS	Engineered Safety Features Actuation System
ESFS	Engineered Safety Feature System
ESW	Essential Service Water
FANP	Framatome Advanced Nuclear Power, Inc.
FBVIS	Fuel Building Ventilation Isolation Signal
FSAR	Final Safety Analysis Report (Callaway Only)
FW	Feedwater
FWIS	Feedwater Isolation Signal
FWIV	Feedwater Isolation Valve
FWLB	Feedwater Line Break
GND	Ground
H2	Hydrogen
HELB	High Energy Line Break
HFP	Hot Full Power

HMI	Human Machine Interface
HVAC	Heating Ventilation and Air Conditioning
I/O	Input/Output
ITDP	Improved Thermal Design Procedure
I&C	Instrumentation and Control
KB	Kilobyte
kV	Kilovolts
LCO	Limiting Condition for Operation
LOCA	Loss-Of-Coolant Accidents
LOP	Loss-Of-Offsite Power
LSELS	Load Shedder and Emergency Load Sequencer
LSSS	Limited Safety System Settings
LVL	Level
M/A	Manual/Automatic
MCB	Main Control Board
MCC	Motor Control Center
MCR	Main Control Room
MSFIS	Main Steam and Feedwater Isolation System
MHz	Megahertz
MMF	Minimum Measured Flow
MSI	Monitoring and Service Interface
MSIV	Main Steam Isolation Valve
MSLB	Main Steam Line Break
MTBF	Mean Time Between Failures
MTTR	Mean Time to Repair
NCP	Normal Charging Pump
NIS	Nuclear Instrumentation System
NMI	Non-Maskable Interrupt
NPP	Nuclear Power Plant
NPSH	Net Positive Suction Head
NR	Narrow Range

NRC	Nuclear Regulatory Commission
NSSS	Nuclear Steam Supply System
OM	Operation and Monitoring System
OM690	Screen-based TXP Operation and Monitoring System
OPΔT	Overpower Delta T
OT	Operator Terminals
OTΔT	Overtemperature Delta T
PAMS	Post Accident Monitoring System
PORV	Power Operated Relief Valve
PU	Processing Unit
PWR	Pressurized Water Reactor
QDS	Qualified Display System
RAM	Random Access Memory
RCCA	Rod Cluster Control Assembly
RCS	Reactor Coolant System
RCP	Reactor Coolant Pump
RFI	Radio Frequency Interference
RG	NRC Regulatory Guide
ROM	Read-Only Memory
RPS	Reactor Protection System (RTS and NSSS ESFAS functions, and other SSPS functions in the original W7300 and SSPS Systems)
RTB	Reactor Trip Breaker
RTD	Resistance Temperature Detector
RTE	Runtime Environment
RTP	Rated Thermal Power
RTS	Reactor Trip System
RVLIS	Reactor Vessel Level Indicating System
RWST	Refueling Water Storage Tank
RX	Reactor
SAA1	Analog Signal Module
SAR	Safety Analysis Report

SBO	Station Blackout
SCP2	TXS Communication Processor for Ethernet Connection
SEQ	Sequencer
SG	Steam Generator
SGBSIS	Steam Generator Blowdown Steam Isolation Signal
SGTR	Steam Generator Tube Rupture
SI	Safety Injection
SIS	Safety Injection Signal
SL	Safety Limit
SLIS	Steam Line Isolation Signal
SPACE	Specification and Coding Environment
SRP	Standard Review Plan
SSC	System Support Controller
SSPS	Solid State Protection System
SU	Server Unit
SVE2	TXS Central Processing Unit
SWCMF	Software Common-Mode Failure
SWPC	Siemens Westinghouse Power Corporation
TC/CCM	Thermocouple Core Cooling Monitor
TDAFP	Turbine Driven Auxiliary Feedwater Pump
TS	Technical Specification
TXP	TELEPERM XP
TXS	TELEPERM XS
USAR	Updated Safety Analysis Report (WCNOC only)
UV	Undervoltage
VAC	Volts Alternating Current
VCT	Volume Control Tank
VDC	Volts Direct Current
WCGS	Wolf Creek Generating Station
WCNOC	Wolf Creek Nuclear Operating Corporation

2 REGULATORY POSITION

NUREG-0800, BTP HICB-19, "Guidance of Evaluation of Defense-in-Depth and Diversity in Digital Computer-Based Instrumentation and Control Systems," (Reference /1/) indicates that Digital I&C systems are vulnerable to common-mode failure caused by software error, which defeats the redundancy achieved by hardware architecture. In NUREG-0493, "A Defense-in-Depth & Diversity Assessment of the RESAR-414 Integrated Protection System" (Reference /8/), the NRC documented a D-in-D&D analysis of a digital computer-based RPS, in which defense against common-mode failures was based upon an approach using a specified degree of system separation and diversity between echelons of defense. Subsequently, in SECY 91-292, "Digital Computer Systems for Advanced Light-Water Reactors" (Reference /21/), the Commission included discussion of its concerns about common-mode failures in digital systems used in nuclear power plants. As a result of the reviews of ALWR design certification applications that used digital protection systems, the Commission documented its position with respect to common-mode failures in digital systems and defense-in-depth. This position was documented as Item II.Q in SECY 93-087, "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs" (Reference /22/), and was subsequently modified in the associated Staff Requirements Memorandum. Based on experience in the detailed reviews, the NRC has established acceptance guidelines for D-in-D&D assessments as described in BTP HICB-19.

2.1 REGULATORY BASES

1. 10 CFR 50.55a(h), "Protection Systems," requires in part that protection systems satisfy the criteria of ANSI/IEEE Std. 279, "Criteria for Protection Systems for Nuclear Power Generating Stations." Section 4.2 requires in part that "any single failure within the protection system shall not prevent proper protective action at the system level when required."

2. 10 CFR 50.62, "Requirements for Reduction of Risk from Anticipated Transients without Scram," requires in part various diverse methods of responding to anticipated transients without scram (ATWS).

3. 10 CFR 50 Appendix A, General Design Criterion (GDC) 21, "Protection Systems Reliability and Testability," requires in part that "no single failure results in the loss of the protection system."

4. 10 CFR 50 Appendix A, GDC 22, "Protection System Independence," requires in part that the effects of natural phenomena, postulated accident conditions, normal operating, maintenance, and testing not result in the loss of protective function. "Design techniques, such as functional diversity or diversity in component design and principles of operation, shall be used to the extent practical to prevent loss of the protection function."

5. 10 CFR 50 Appendix A, GDC 24, "Separation of Protection and Control Systems," requires in part that "Interaction of the protection and control systems shall be limited so as to assure that safety is not significantly impaired."
6. 10 CFR 50 Appendix A, GDC 29, "Protection Against Anticipated Operational Occurrences," requires in part defense against anticipated operational transients "to assure an extremely high probability of accomplishing safety functions."

2.2 REGULATORY GUIDANCE

1. Regulatory Guide 1.53, "Application of the Single-Failure Criterion to Nuclear Power Plant Protection Systems," clarifies the application of the single-failure criterion (GDC 21) and endorses ANSI/IEEE Std. 379, "Standard Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems," providing supplements and an interpretation.

2. Regulatory Guide 1.153, "Criteria for Safety Systems," endorses IEEE Std. 603, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," as an alternative to ANSI/IEEE Std. 279.

3. NUREG-0493 "A Defense-in-Depth & Diversity Assessment of the RESAR-414 Integrated Protection System," is the first formal D-in-D&D assessment of a RPS, the RESAR-414.

4. NUREG/CR-6303, "Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems," documents several D-in-D&D analyses performed after 1990, and presents a method for performing such analyses.

5. The Staff Requirements Memorandum on SECY 93-087 describes the NRC position on D-in-D&D.

2.3 BRANCH TECHNICAL POSITION HICB-19

As a result of the reviews of ALWR design certification applications that used digital protection systems, the NRC established the following position on D-in-D&D for the advanced reactors. Items 1, 2, and 3 of this position apply to digital system modifications to operating plants.

1. The applicant/licensee should assess the D-in-D&D of the proposed I&C system to demonstrate that vulnerabilities to common-mode failures have been adequately addressed.

2. In performing the assessment, the vendor or applicant/licensee shall analyze each postulated common-mode failure for each event that is evaluated in the accident analysis section of the safety analysis report (SAR), using best-estimate methods. The

vendor or applicant/licensee shall demonstrate adequate diversity within the design for each of these events.

3. If a postulated common-mode failure could disable a safety function, then a diverse means should be required to perform either the same function or a different function, with a documented basis that the diverse means is unlikely to be subject to the same common-mode failure. The diverse or different function may be performed by a non-safety system, if the system is of sufficient quality to perform the necessary function under the associated event conditions.

4. A set of displays and controls located in the main control room should be provided for manual system-level actuation of critical safety functions and monitoring of parameters that support the safety functions. The displays and controls should be independent and diverse from the safety computer systems identified in items 1 and 3 above.

The additional manual capability required by Item 4 is considered necessary in advanced reactors because all of the protection and control systems, including portions of the manual actuation paths typically are digital computer-based, and thus potentially vulnerable to common-mode failure.

The above position is based on the NRC position that software design errors are a credible source of common-mode failures. The NRC position is that software cannot be proven to be error-free, and therefore is considered susceptible to common-mode failures because identical copies of the software are present in redundant channels of safety related systems. To defend against potential common-mode failures, the NRC considers high quality, diversity, and defense-in-depth, to be key elements in digital system design. High-quality software and hardware reduces failure probability. However, despite high quality of design, the NRC position is that software errors may still defeat safety functions in redundant, safety related channels. Therefore, as set forth in Items 1, 2, and 3 above, the NRC requires that the applicant/licensee perform a D-in-D&D assessment of the proposed digital I&C system to demonstrate that vulnerabilities to common-mode failures have been adequately addressed. In this assessment, the applicant/licensee must evaluate design basis events (as identified in the SAR). If a postulated common-mode failure can disable a safety function that is required to respond to the design basis event being analyzed, then a diverse means of effective response (with documented basis) is necessary. The diverse means may be a non-safety system, automatic, or manual if the system is of sufficient quality to perform the necessary function under the associated event conditions and within the required time.

As described in Appendix 7.0-A of BTP HICB-19, the D-in-D&D assessment is only required for digital RTS and ESFAS replacements. However, credit cannot be given for any system, safety or non-safety related, vulnerable to the same software common-mode failure. For this reason, special attention is given to the BOP ESFAS, ESFAS support systems, and control systems that are being upgraded to the TXS system to ensure that credit is not given for their operability if the same common-mode failure could affect their operability. EPRI TR-102348, Revision 1, "Guidelines on Licensing Digital Upgrades" (Reference /3/), provides additional guidance on D-

in-D&D assessments. This guidance was endorsed by the NRC (Reference /4/) and used in the development of this report to aid in the establishment of certain boundaries.

2.4 ACCEPTANCE CRITERIA

Based on experience in detailed reviews, the NRC has established acceptance guidelines for D-in-D&D assessments.

The D-in-D&D assessment submitted by the applicant/licensee should demonstrate compliance with the NRC's position. To reach a conclusion of acceptability, the following four conclusions should be reached and supported by summation of the results of the assessment:

1. For each anticipated operational occurrence in the design basis occurring in conjunction with each single postulated common-mode failure, the plant response calculated using best-estimate (realistic assumptions) analyses should not result in radiation release exceeding 10% of the 10 CFR 100 guideline value, or violation of the integrity of the primary coolant pressure boundary. The applicant/licensee should either (1) demonstrate that sufficient diversity exists to achieve these goals, or (2) identify the vulnerabilities discovered and the corrective actions taken, or (3) identify the vulnerabilities discovered and provide a documented basis that justifies actions not taken.

2. For each postulated accident in the design basis occurring in conjunction with each single postulated common-mode failure, the plant response calculated using best-estimate (realistic assumptions) analyses should not result in radiation release exceeding the 10 CFR 100 guideline values, violation of the integrity of the primary coolant pressure boundary, or violation of the integrity of the containment (i.e., exceeding coolant system or containment design limits). The applicant/licensee should either (1) demonstrate that sufficient diversity exists to achieve these goals, or (2) identify the vulnerabilities discovered and the corrective actions taken, or (3) identify the vulnerabilities discovered and provide a documented basis that justifies actions not taken.

3. When a failure of a common element or signal source shared between the control system and the RTS is postulated, and (1) this common-mode failure results in a plant response that requires reactor trip, and (2) the common-mode failure also impairs the trip function, then diverse means that are not subject to or failed by the postulated failure should be provided to perform the RTS function. The diverse means should ensure that the plant response calculated using best-estimate (realistic assumptions) analyses does not result in radiation release exceeding 10% of the 10 CFR 100 guideline value, or violation of the integrity of the primary coolant pressure boundary.

   When a failure of a common element or signal source shared between the control system and the ESFAS is postulated, and (1) this common-mode failure results in a plant response that requires ESF, and (2) the common-mode failure also impairs the

ESF function, then diverse means that are not subject to or failed by the postulated failure should be provided to perform the ESF function. The diverse means should ensure that the plant response calculated using best-estimate (realistic assumptions) analyses does not result in radiation release exceeding 10% of the 10 CFR 100 guideline value, or violation of the integrity of the primary coolant pressure boundary.

Interconnections between reactor trip and ESFAS for interlocks providing for (1) reactor trip if certain engineered safety features (ESFs) are initiated, (2) ESF initiation when a reactor trip occurs, or (3) operating bypass functions, are permitted provided that it can be demonstrated that functions required by the ATWS rule (10 CFR 50.62) are not impaired.

4. No failure of monitoring or display systems should influence the functioning of the RTS or the ESFAS. If plant monitoring system failure induces operators to attempt to operate the plant outside safety limits or in violation of the limiting conditions of operation, the analysis should demonstrate that such operator-induced transients will be compensated by protection system function

The adequacy of the diversity provided with respect to the above criteria must be justified. Section 3.2 of NUREG/CR-6303 describes six types of diversity and describes how instances of different types of diversity might be combined into an overall case for the sufficiency of the diversity provided. Typically, several types of diversity should exist, some of which should exhibit one or more of the stronger attributes listed in NUREG/CR-6303 for the diversity type.

The justification for equipment diversity, or for the diversity of related system software such as a real-time operating system, must extend to the equipment's components to ensure that actual diversity exists. For example, different manufacturers might use the same processor or license the same operating system, thereby incorporating common failure modes. Claims for diversity based just on difference in manufacturer name are insufficient without consideration of the above.

3 ASSESSMENT METHODOLOGY

The D-in-D&D assessment presents the qualitative results using best-estimate methods for all selected events in accordance with current regulatory guidance and methodology and defines the D-in-D&D functional requirements for the Callaway Plant and WCGS.

3.1 ECHELONS OF DEFENSE-IN-DEPTH

The NRC has identified four echelons of defense against common-mode failures. The I&C systems included in the four echelons of defense-in-depth consist of:

1. the Control System,
2. the RTS,
3. the ESFAS, and
4. the Monitoring and Indication System.

These four echelons are ranked according to the preferred mode for handling an incident. First, the control systems are the preferred method to use to handle any event, as they are in normal use throughout the plant cycle. The RTS is next, in that it is actuated to prevent any reactivity excursion, and third, the ESFAS is used to mitigate any event that has not been handled by the first two echelons. The Monitoring and Indication Systems are the last echelon and provide the operator with the means to manually control the plant. These four echelons provide the defense-in-depth necessary to cope with a variety of accidents, transients and abnormal operating occurrences. This I&C system ranking follows the guidance presented in References /1/, /8/, and /10/.

Descriptions reflecting the current system designs are described in the FSAR Chapter 7 (Reference /5/) and USAR Chapter 7 (Reference /24/). Descriptions of the current system and changes resulting from the proposed I&C digital upgrade and their effects on D-in-D&D are described in Section 4 of this assessment.

In the defense-in-depth concept of the plant, the control systems, the RTS, the ESFAS, and Monitoring and Indication Systems represent the main line of defense. A second line of defense is provided by a combination of control systems, the AMSAC, and independent manual controls. Although considered incredible, in event that RTS and/or ESFAS are unavailable due to a hypothetical postulated software common-mode failure, the architecture of the digital I&C upgrade has been carefully designed to assure that the control systems, AMSAC, and indications necessary for operator action remain available. In Section 5, it will be shown that the TXS architecture and certain features have been designed to eliminate the failure of safety functions due to software common-mode failures.

3.2 EVALUATING DIVERSITY-SYSTEM REPRESENTATION AS BLOCKS

To determine diversity within the different TXS systems, it is partitioned into blocks/modules in accordance with NUREG/CR-6303, Section 2.5 (Reference /10/) and NUREG-0493 (Reference /8/). These blocks/modules represent diverse software or equipment/modules. Vulnerability to common-mode failures and diversity within the TXS system is determined at this level.

Using the guidance provided in NUREG/CR-6303 (APPENDIX-BLOCK EXAMPLES), the digital-based RTS, NSSS ESFAS, and BOP ESFAS functions and other TXS based safety functions, such as MSFIS, EDG controls, LSELS, Class 1E Analog Controls, TC/CCM, RVLIS, and Qualified Display System that are processed by the TXS system, are evaluated for diversity and independence from each other.

The adequacy of the diversity provided between the TXS, TXP and any other system credited for diversity are assessed. NUREG/CR-6303 Section 3.2 describes six types of diversity and describes how instances of different types of diversity might be combined into an overall case for the sufficiency of the diversity provided. Typically, several types of diversity will be shown to exist, some of which should exhibit one or more of the stronger attributes listed in NUREG/CR-6303 for the diversity type.

Section 6 examines aspects of high integrity design that contribute to TXS system dependability: aspects pertaining to quality, design, reliability, availability, and configuration control. Section 6 also discusses quality as it relates to the diverse non-safety related TXP system.

A more detailed discussion of diversity within the design of the individual TXS systems is presented in Section 5; diversity between TXS and TXP systems is presented in Section 7.

Finally, this assessment examines each of the design basis events identified in the accident analysis section of the FSAR/USAR and the impact of software common-mode failures on the safety analysis.

3.3 TYPES OF DIVERSITY ASSESSED

The TXS systems are partitioned into blocks in accordance with NUREG/CR-6303, Section 2.5. Diversity is determined at the block level. The different forms of diversity to be assessed are:

- Design Diversity
- Equipment Diversity
- Software Diversity
- Functional Diversity
- Signal Diversity
- Human Diversity

The FANP D-in-D&D methodology credits the inherent diversity within the design of the individual TXS system, between the TXS and TXP system and between TXS system and other equipment.

3.4 FAILURE TYPES

NUREG/CR-6303 (Guideline 3) describes three different instrument failure types. The assessment will evaluate the design techniques used in the TXS system to cope with these failures:

Type 1 Failure:
Type 1 failures are postulated failures in one echelon that result in a plant transient that requires a protection function to mitigate the transient. Generally, the postulated failure is assumed to occur in the control system echelon such that a plant transient occurs that results in an automatic reactor trip or ESF actuation. However, there are some postulated failures in the ESF (due to interconnections and interlocks between the ESFAS and RTS echelon) that necessitate protective action.

Type 2 Failure:
Type 2 failures are undetected failures that are manifested only when a demand is received to actuate a component or system. Failure to respond is due to a postulated common-mode failure of redundant divisions or trains.

Type 3 Failure:
Type 3 failures are failures that occur because either the plant process does not respond in a predictable manner or the sensors measuring the plant process respond in an anomalous manner.

3.5 DOCUMENTATION OF ASSUMPTIONS

The D-in-D&D methodology utilizes the following assumptions for interpretation of the assessment guidelines:

1. Hardware failures associated with environmental, seismic, and EMI/RFI are excluded as plausible common-mode failures to the TXS-based components based on qualification of components per Topical Report EMF-2110(NP), Reference /2/ and the TXS safety evaluation, Reference /29/.

2. When a failure is assumed for a block, reactor trip and/or ESF actuations associated with this block and associated components downstream of the failure may not activate.

3. If the action credited to mitigate the consequences of the postulated accident is assumed to fail either high or low, due to a block failure, then it is acceptable to conclude that all other actuations associated with the failed block will fail in the same direction. It

is not a requirement to assume "smart" failures or the worst possible combination of all postulated failures.

4. Safety actuation channels that are not credited in the accident analysis to provide protection for the postulated event under assessment, will not fail in a manner to worsen the consequences.

The validity of the above assumptions is discussed in NUREG/CR-6303 and will be explored in more detail in Section 5 (TXS System Architecture and System Diversity) and Section 7 (Defense-in-Depth and Diversity).

3.6 FSAR/USAR Event Specific Evaluation Process

In accordance with the methodology prescribed in BTP HICB-19, this assessment examines each of the design basis events identified in the accident analysis section of the FSAR/USAR. All the events described in FSAR/USAR Chapter 15 are evaluated. Several other accidents are also considered relevant for this evaluation. They are the containment functional design described in FSAR/USAR Chapter 6.2.1, and the equipment environmental qualification issues described in FSAR/USAR Chapter 3.0. Together, these events are considered to be the full set of events that need to be considered in assessing the impact of common-mode failures on the safety analysis.

If a postulated common-mode failure could disable a safety function that is required to respond to the design basis event being analyzed, then a diverse means, from one of the above four echelons of defense, of effective response (with documented basis) is necessary. The diverse means may be a safety or non-safety system, automatic, or manual, if the system is of sufficient quality to perform the necessary function under the associated event conditions and within the required time. Any system credited as a defense-in-depth system has to be diverse from the TXS based RTS and/or ESFAS and not subject to the same common-mode failure.

For each common software element between the control system and the RTS or the ESFAS, the failure of this element is postulated, and an assessment is performed to show that a diverse means exists, not subject to the same failure, such that the conditions as outlined above are still met. Any other safety or non-safety related system subject to the same common-mode failure cannot be credited as a valid diverse means.

[

] On the basis that no safety functions are disabled by the worst-case common-mode failure, the outcome of re-evaluating all of the accidents and transients analyzed in the FSAR/USAR could be anticipated. Nevertheless, for completeness of analysis and in

accordance with BTP HICB-19 guidance, a complete qualitative re-evaluation of the events analyzed in the FSAR/USAR was performed.

3.6.1 Assessment Goals and Tasks

The goals of the Callaway Plant and WCGS assessment is to implement the NRC's positions cited in BTP HICB-19, to determine and correct vulnerability to undetected common-mode failures occurring with design basis events, and to ensure that operators have enough diverse instrumentation to follow proper and acceptable manual actions. Effects of the combined failure, the common-mode failure and the failure causing the event, including the event sequence, are reviewed using "best estimate" methods and realistic assumptions. The results of this assessment are discussed in Section 8.

The defense-in-depth strategy has been devised to satisfy NRC acceptance criteria while achieving three primary implementation goals:

1. No requirement to perform new FSAR/USAR Chapter 15 accident analysis. An assessment of the existing safety analysis and associated assumptions should be adequate.

2. No requirement to add or expand diverse actuation systems. With a skillful arrangement of diverse I&C equipment, it should be unnecessary to burden the plant with requirements to add new diverse actuations or to expand an existing diverse system such as AMSAC.

3. No requirement to add new diverse indications or manual controls. With a skillful arrangement of I&C equipment, it should be possible to preserve the integrity of signals to control systems and post accident monitoring indications, even in the presence of an unlikely software common-mode failure.

The tasks used to evaluate the impact of common-mode failure for each FSAR/USAR event are summarized below:

Task 1:
Determine a realistic sequence of events. Note that the sequence of events for each event as shown in the FSAR/USAR is based on conservative assumptions (loss of offsite power, single failure, etc.). Hence this task relies on prior experience and judgment in combination with the guidance of BTP HICB-19 (Reference /1/) to arrive at a more realistic sequence of events.

Task 2:
Assess the impact of TXS vulnerabilities on the sequence of events. The main objective is to determine the timing of occurrence of key phenomena that would impact the progression of the accident scenario. Examples would be a) beginning of core heatup in a loss of coolant accident (LOCA) event, and b) beginning of fuel failure in a rod ejection event.

Task 3:
Based upon the above impact, determine what operator actions would be necessary to mitigate the accident without exceeding acceptance criteria. One issue would be to determine whether the current acceptance criteria as listed in the FSAR/USAR should still be maintained, or whether alternate acceptance criteria should be proposed. This is common practice for accidents that are considered beyond the design basis of the plant, such as severe accidents. This could have a significant effect on the time available for the operator to recover the plant. In the scope of work reported here, the current acceptance criteria for each of the FSAR/USAR events are assumed. Exceptions are noted. The exceptions include a) no significant fuel damage (W-3 DNBR > 1), and b) reactor coolant system (RCS) pressure less than ASME Boiler and Pressure Vessel Level C service limits. These criteria have been used in generic ATWS analysis (References /25/ and /26/) and are used in specific FSAR/USAR events when appropriate. These exceptions are also consistent with the guidance of BTP HICB-19 (Reference /1/).

Task 4:
Compare the results of the best-estimate assessment to acceptance criteria. The results of the evaluation are presented in Section 8 of this report.

3.6.2 Realistic Assumption Conditions

For the assessments performed, allowance is given to use "Best Estimate/Realistic Assumptions" in conformance with BTP HICB-19 (Reference /1/). Initial plant conditions considered in the assessment included normal conditions defined by ANS Condition I – Normal Operation and Operational Transients. Allowances for uncertainties in plant parameters were omitted for the software common-mode failure evaluations. Nominal plant operating conditions at 100% rated thermal power included:

Callaway Plant:

- NSSS Thermal Power – 3579 MWt (FSAR Table 15.0-3)
- RCS Coolant Flow – 382,630 gpm MMF (FSAR Table 15.0-3)
- RCS Coolant Flow – 141.9 x 10^6 lb/hr MMF (FSAR Table 15.0-3)
- Thermal Power Generated by reactor coolant pumps (RCPs) – 14 MWt (FSAR Table 15.0-1)
- Rated Core Thermal Power – 3565 MWt (FSAR Table 15.0-1)
- HFP Core Inlet Temperature – 557.5°F ITDP (FSAR Table 15.0-3)
- HFP Vessel Average Temperature – 588.4°F (FSAR Table 15.0-3)
- Pressurizer Pressure – 2250 psia (FSAR Table 15.0-3)
- RCS Core Pressure – 2280 psia (FSAR Table 15.0-3)
- Equivalent Steam Generator (SG) Tube Plugging Level (all loops) – 15% (FSAR Table 15.0-2)
- NSSS Steam Flow – 15.91 x 10^6 lb/hr with 15% SG tube plugging (FSAR Table 15.0-3)
- Steam Pressure at SG Outlet – 939 psia with 15% tube plugging (FSAR Table 15.0-3)

- Maximum Steam Moisture Content – 0.25% (FSAR Table 15.0-3)
- Feedwater Temperature at SG Inlet – 446°F with 15% SG tube plugging (FSAR Table 15.0-2)

WCGS:

- NSSS Thermal Power – 3579 MWT (USAR Table 15.0-1)
- RCS Coolant Flow – 90,324 gpm per loop (USAR Table 15.0-3)
- Thermal Power Generated by RCPs – 14 MWt (USAR Table 15.0-1)
- Rated Core Thermal Power – 3565 MWt (USAR Table 15.0-1)
- Core Inlet Temperature – 555.8°F (USAR Table 15.0-3)
- Vessel Average Temperature – 588.4°F (USAR Table 15.0-3)
- RCS Pressure – 2250 psia (USAR Table 15.0-3)
- SG Tube Plugging – 10% (USAR Table 15.0-3)
- NSSS Steam Flow – 15.92 x 10^6 lb/hr (USAR Table 15.0-3)
- Steam Pressure at SG Outlet – 944 psia (USAR Table 15.0-3)
- Maximum Steam Moisture Content – 0.25% (USAR Table 15.0-3)
- Assumed Feedwater Temperature at SG Inlet – 446°F (USAR Table 15.0-2)

Initial values for core power, average RCS temperature and pressurizer pressure were selected as being the normal conditions for the particular plant situation. Steam generator tube plugging was assumed to be within Technical Specification (TS) limits and considered realistic. Concurrent events do not have to be assumed, as the software common-mode failure in conjunction with a single event is highly unlikely. Concurrent events coupled with the software common-mode failure are too unlikely to be considered. Also, a common-mode failure is not assumed to occur in conjunction with a loss of offsite power event and another event initiated such as a steam generator tube rupture (SGTR).

Using a "Best Estimate" evaluation methodology, the setpoints of all functions (except those defeated by common-mode failure) are assumed to trip at the actual setpoint rather than a conservative value such as the analysis limit value. This lessens an inherent conservatism within the Chapter 15 analyses. This implies that the trips and actuations will occur as designed without failures or worse case allowance for uncertainties within the safety related instrumentation loops. All control systems, except those whose failure initiated the event, are considered operable and can aid in the mitigation of the consequences of the event.

Event acceptance criteria used in assessing the impact of postulated common-mode failures included:

Callaway Plant:

- Reactor Coolant Pressure Limit-Service Level C – 3200psig (generic ATWS analyses; References [25] and [26])
- Pressurizer water level Limit – No liquid relief through pressurizer safety valves (FSAR Section 15.5.1, Inadvertent ECCS Actuation)
- Containment Pressure Limit – 60 psig (FSAR Table 6.2.1-2)

- Minimum Departure from Nucleate Boiling Ration (DNBR) – W3 > 1 (generic ATWS analyses; References [25] and [26])
- Clad Temperature Limit – 2700°F (clad integrity and limit on Zirconium-Steam reaction; FSAR Sections 15.3.3, Locked Rotor, and 15.3.4, RCP Shaft Break)
- UO_2 pellet enthalpy at the hot spot – < 200 cal/gm (FSAR Section 15.4.8, Rod Cluster Control Assembly Ejection Accident)
- Main Steam System Pressure Limit – 110% of Design (FSAR Section 15.2.3, Turbine Trip)

WCGS:

- Reactor Coolant Pressure Limit-Service Level C – 3200psig (generic ATWS analyses; References [25] and [26])
- Pressurizer water level Limit – No liquid relief through pressurizer safety valves (FSAR Section 15.5.1, Inadvertent ECCS Actuation)
- Containment Pressure Limit – 60 psig (USAR Table 6.2.1-2)
- Minimum DNBR – W3 > 1 (generic ATWS analyses; References [25] and [26])
- Clad Temperature Limit – 2700°F (clad integrity and limit on Zirconium-Steam reaction; FSAR Sections 15.3.3, Locked Rotor, and 15.3.4, RCP Shaft Break)
- UO_2 pellet enthalpy at the hot spot (for irradiated fuel) – < 200 cal/gm (USAR Section 15.4.8, Rod Cluster Control Assembly Ejection Accident)
- Main Steam System Pressure Limit – 110% of Design (USAR Section 15.2.3, Turbine Trip)

3.6.3 Operator Actions

Plant specific Emergency Operating Procedures (EOPs)/Emergency Procedures (EMGs) for Westinghouse NSSS reactors are formatted similar to the Emergency Response Guidelines (ERGs), which are written and supplied by the Westinghouse Owners Group (WOG). Upon detecting symptoms requiring a reactor trip or safety injection, operators will enter EOP/EMG E-0, REACTOR TRIP OR SAFETY INJECTION. In step 1 of E-0, the operator is required to manually trip the reactor if the trip has not occurred. In step 4, the operator is required to manually actuate safety injection if it is required and has not occurred. New EOPs/EMGs and new operator training are not required. This evaluation assumes that the common-mode failure does not also disable the indications and controls used by the operator to detect symptoms and complete manual actions.

In designing for and analyzing for a DBA (i.e., LOCA, MSLB, FHA, or SGTR), no operator action is assumed to be taken by plant operators to correct problems during the first 10 minutes following the accident (Reference FSAR/USAR Section 3.1.2, "Additional Single Failure Assumptions"). Although not a design basis accident, operator action times of less than 10 minutes are also assumed in the mitigation of an inadvertent ECCS actuation at power event.

The following approach is used for evaluating the impact of common-mode failure on the FSAR/USAR events. For those events where credit for operator action in less than 10 minutes is required to meet acceptance criteria, this will be clearly identified so that further validation can be provided.

As mentioned previously, the FSAR/USAR event evaluations provided in this report assume that the common-mode failure does not disable the indications and controls used by the operator. Instrumentation used by operators to monitor symptoms requiring reactor trip or ESFAS actuation are provided by EOP/EMG E-0, REACTOR TRIP OR SAFETY INJECTION. The list is extracted from EOP/EMG E-0 and shown below:

- Source range neutron flux
- Intermediate range neutron flux
- Power range neutron flux
- Power range neutron flux high positive rate
- OverTemperature Delta T (OTΔT)
- OverPower Delta T (OPΔT)
- Pressurizer pressure
- Pressurizer water level
- RCS Flow
- SG NR water level
- RCP Undervoltage
- RCP Underfrequency
- Turbine trip low fluid oil pressure
- Turbine trip stop valve closure
- Containment pressure
- Steam line pressure

EOP/EMG E-0 is assumed to provide the entry point into emergency procedures for operator response to events discussed in this section.

3.7 CONCLUSIONS

Results of re-evaluating the accidents and transients analyzed in the FSAR/USAR (assuming a concurrent common-mode failure) are summarized in Section 8. Conclusions for the overall D-in-D& D assessment are presented in Section 9.

4 CALLAWAY PLANT AND WOLF CREEK GENERATING STATION INTEGRATED DIGITAL DESIGN

The TXS system as described in Topical Report EMF-2110 (NP), Revision 1, "TXS: A Digital Reactor Protection System" (Reference /2) will replace the present safety related I&C systems. Although the topical report emphasizes the RTS and ESFAS functions, the TXS design concepts are applicable to all TXS safety related I&C systems. The plant-specific open items listed in the Topical Report will be addressed during the licensing phase for each system. This assessment addresses only one of these open items, D-in-D&D. This report also discusses selected non-safety related control systems that will be upgraded using the TXP system. A graphical representation of the I&C Distributed Control System (DCS) Upgrade is shown in (Figure 4-1).

4.1 OVERVIEW OF DCS UPGRADE

4.1.1 Scope of Safety I&C DCS Upgrade

The TXS system is to be used to upgrade the safety related I&C systems described in the following sections of the FSAR/USAR:

- Section 7.2, Reactor Trip System
- Section 7.3, Engineered Safety Feature Systems
- Section 7.4, Systems Required for Safe Shutdown
- Section 7.5, Safety-Related Display Instrumentation
- Section 7.6, Other Instrumentation Systems Required for Safety

The safety related DCS will also upgrade the following safety related systems:

- LSELS
- EDG

The TXS systems will perform all of the functions currently implemented in the W7300 Process Protection Sets, NIS, and the Solid-State Protection System. Other TXS systems will perform the BOP ESFAS functions, the LSELS, the MSFIS, EDG Controls, Class 1E Analog Control functions, TC/CCM, and RVLIS.

In addition, a Class 1E Qualified Display System is provided with flat screens which are used for the display and short term trend display of Post Accident Monitoring System (PAMS) Regulatory Guide 1.97 variables, RVLIS, and TC/CCM. Normal plant control functions will be performed using systems diverse from the TXS system such as the TXP system.

4.1.2 Scope of Non-Safety I&C DCS Upgrade

The TXP system is to be used to upgrade non-safety related instrumentation and control systems described in Section 7.7 of the FSAR/USAR:

The TXP system will provide all of the functions currently implemented in the NSSS and BOP control systems for Reactor Control, Rod Control, and control system Interlocks, Pressurizer Pressure Control, Pressurizer Water Level Control, SG Water Level Control, Steam Dump Control, and Incore Instrumentation monitoring. The TXP system will also perform the AMSAC functions as well as provide additional manual diverse control functions. The TXP system also performs functions not discussed in this report. This report only discusses the TXP systems credited for D-in-D&D.

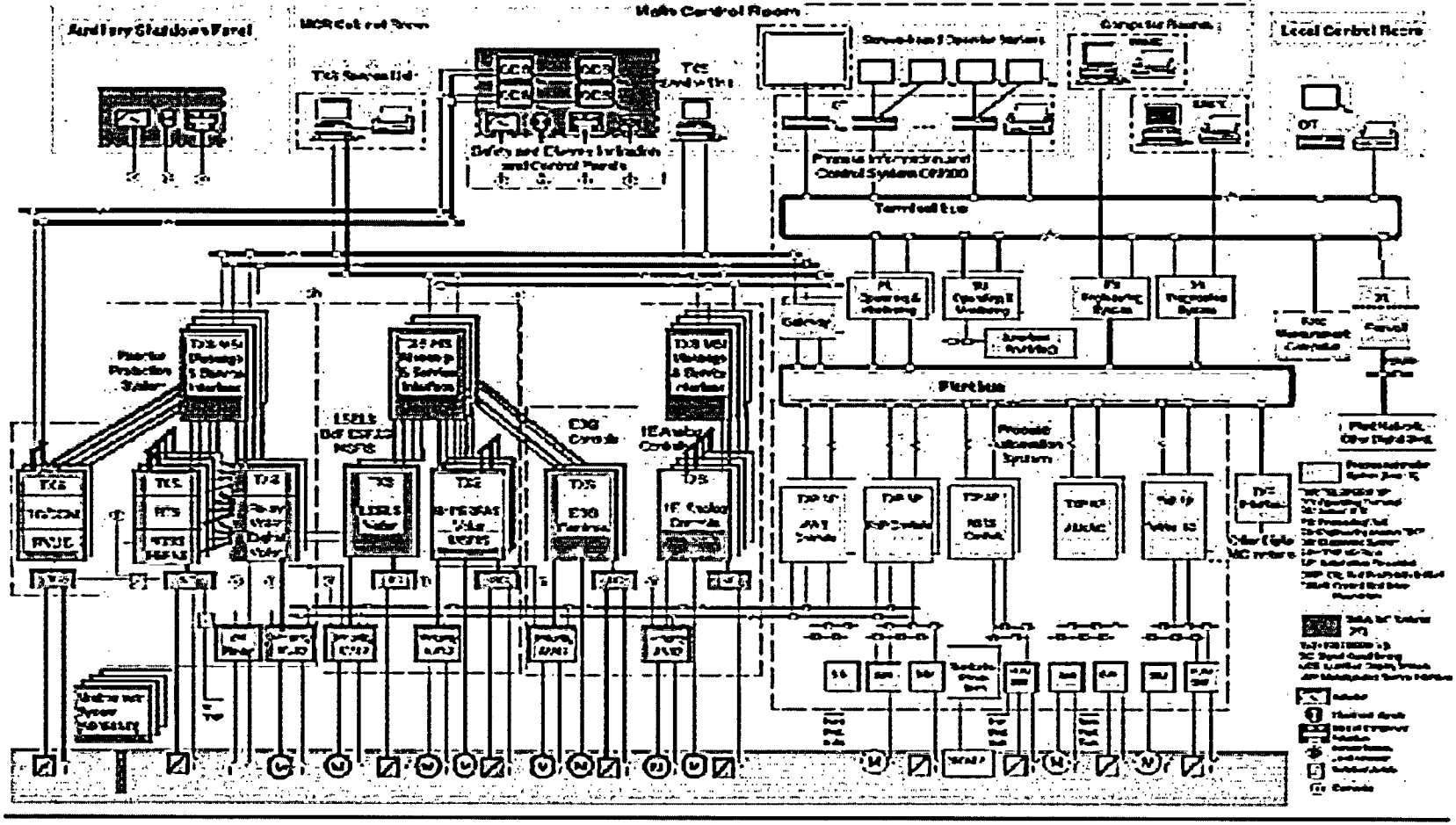


Figure 4-1: Architecture of the Callaway and WCGS DCS I&C Systems

4.2 CURRENT RTS, ESFAS, AND LSELS

The current design combines the RTS, NIS inputs, Turbine Trip inputs, NSSS ESFAS functions, BOP ESFAS functions, MSFIS functions, and LSELS functions into an integrated system. A block diagram of the current RTS, ESFAS, and LSELS is shown in Figure 4-2.

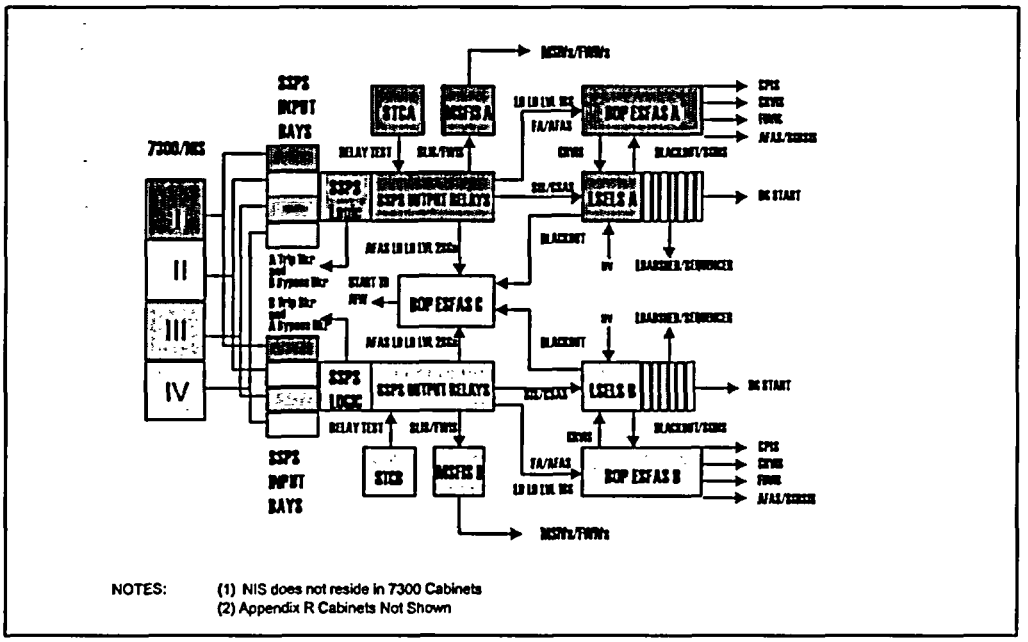


Figure 4-2: Current RTS, ESFAS, and LSELS

4.2.1 Current Reactor Trip System (RTS) Instrumentation Functions

4.2.1.1 Current RTS Functions

The information about which systems are considered part of RTS is provided in the FSAR/USAR Section 7.2 (Reference /5/ and /24/). The RTS consists of those instrumentation systems which automatically shutdown the plant when the reactor is approaching operation outside the limits of its safe operating region. The following systems currently make up the RTS:

- W7300 Process Instrumentation and Control System
- NIS
- Solid State Protection System (SSPS)
- Reactor Trip Switchgear (not shown on Figure 4-2)
- Manual Actuation Circuits (not shown on Figure 4-2)

The RTS initiates a unit shutdown, based on the values of selected unit parameters, to protect against violating the core fuel design limits and RCS pressure boundary during anticipated operational occurrences and to assist the ESF Systems in mitigating accidents.

The RTS instrumentation is segmented into four distinct but interconnected modules as described in FSAR/USAR, Chapter 7 (Reference /5/and /24/), and as identified below:

1. Field transmitters or process sensors: provide a measurable electronic signal based upon the physical characteristics of the parameter being measured;

2. The current signal process control and protection system includes the 7300 Process Protection System, NIS, field contacts, and protection channel sets. It provides signal conditioning, bistable setpoint comparison, and process algorithm actuation, compatible electrical signal output to protection system devices, and control board/main control room /miscellaneous indications.

3. The current SSPS, including input, logic, and output bays, is used to initiate proper unit shutdown and/or ESF actuation in accordance with the defined logic, which is based on the bistable outputs from the signal process control and protection system.

4. Reactor trip switchgear, including reactor trip breakers and bypass breakers: provides the means to interrupt power to the control rod drive mechanisms and allows the rod cluster control assemblies, or "rods," to fall into the core and shut down the reactor. The bypass breakers allow testing of the reactor trip breakers at power.

The SSPS takes binary inputs (voltage/no voltage) from the process and nuclear instrument channels corresponding to conditions (normal/abnormal) of plant parameters. The system combines these signals in the required logic combination and generates a trip signal (no voltage) to the undervoltage coils of the reactor trip breakers when the necessary combination of signals occurs. This trip signal also de-energizes the auto shunt trip relay which, in turn, closes a contact that energizes the shunt trip coil. The system also provides annunciator, status light, and computer input signals which indicate the condition of bistable input signals, partial trip and full trip functions, and the status of the various blocking, permissive, and actuation functions. In addition, the system includes means for semiautomatic testing of the logic circuits.

4.2.1.2 Current Nuclear Instrumentation System Functions

The primary function of nuclear instrumentation is to protect the reactor by monitoring the neutron flux and generating appropriate trips and alarms for various phases of reactor operating and shutdown conditions. The instrumentation also provides a secondary control function and indicates reactor status during startup and power operation. The NIS uses information from three separate types of instrumentation channels to provide three discrete protection levels. Each range of instrumentation

(source, intermediate, and power) provides the necessary overpower reactor trip protection required during operation in that range. The system provides main control room indication and recording of signals proportional to reactor neutron flux during core loading, shutdown, startup, and power operation, as well as during subsequent refueling. Startup rate indication for the source and intermediate range channels is provided at the control board. Reactor trip, control rod stop, and control and alarm signals are transmitted to the reactor control and protection systems. Equipment failures and test status information are annunciated in the main control room.

Various process signals are taken from sensors both inside and outside containment and sent to the 7300 Protection racks. These signals are conditioned for their specific use and may be sent to either the SSPS or to the 7300 Control racks. Should a parameter have an associated control and protective function, the control function is electronically isolated from the protective function to prevent a failure in the 7300 control system from causing a failure in the protection system. Meters, recorders, alarms and components controlled by the 7300 control systems are only isolated from the 7300 Process Protection System.

The NIS power range detectors are located external to the reactor vessel and measure neutrons leaking from the core. The NIS power range detectors provide input to the Rod Control System and the SG Water Level Control System. Therefore, the actuation logic must be able to withstand an input failure to the control system, which may then require the protection function actuation, and a single failure in the other channels providing the protection function actuation. Note that this function also provides a signal to prevent rod withdrawal prior to initiating a reactor trip. Limiting further rod withdrawal may terminate the transient and eliminate the need to trip the reactor.

4.2.1.3 Current Turbine Trip Instrumentation System Functions

The reactor trip on a turbine trip is actuated by two-out-of-three logic from emergency trip fluid pressure signals or by all closed signals from the turbine steam stop valves. This trip is included as part of good engineering practice. The reactor trip on turbine trip provides additional protection and conservatism beyond that required for the health and safety of the public, practice and prudent design. The turbine provides anticipatory trips to the RPS from contacts which change position when the turbine stop valves close or when the turbine emergency trip fluid pressure goes below its setpoint. The SSPS cabinets are provided with fuse protection for the turbine stop valve reactor trip cabling in the Turbine Building to preclude degradation of required SSPS functions. Faults on the Turbine Building cables going to the oil pressure low transmitters will not degrade the protection system as they are isolated from the protection system by the process instrumentation (Foxboro) cabinets in the main control room.

4.2.2 Current Engineered Safety Features Actuation System (ESFAS) Instrumentation Functions

The information about which systems are considered part of ESFAS is provided in the FSAR/USAR Section 7.3 (Reference /5/ and /24/). The ESFAS are those instrumentation systems outside RTS that are needed to actuate the equipment and systems required to mitigate the consequences of postulated design basis accidents. The ESFAS functions and its support systems include the following:

ESFAS functions:

- Containment Combustible Gas Control (FSAR/USAR Section 7.3.1)
- Containment Purge Isolation (FSAR/USAR Section 7.3.2)
- Fuel Building Ventilation Isolation (FSAR/USAR Section 7.3.3)
- Control Room Ventilation Isolation (FSAR/USAR Section 7.3.4)
- Auxiliary Feedwater Supply (FSAR/USAR Section 7.3.6)
- Main Steam and Feedwater Isolation (FSAR/USAR Section 7.3.7)
- NSSS ESFAS Safety Injection (actuated devices are listed in FSAR/USAR Section 7.3.8.1.1h.)

BOP ESFAS support systems:

- Containment Atmosphere Monitoring System (FSAR/USAR Section 7.3.1.1.1.i)
- 125 VDC Power Supplies (FSAR/USAR Sections 7.3.2.1.1.i, 7.3.3.1.1.i, 7.3.6.1.1.h, and 7.3.7.1.1.h)
- Instrument Air System (FSAR/USAR Sections 7.3.2.1.1.i, 7.3.3.1.1.i, and 7.3.7.1.1.h)
- Vital Class 1E AC Electrical Power System (FSAR/USAR Sections 7.3.1.1.1.i, 7.3.4, and 7.3.6.1.1.h
- Auxiliary Feedwater (AFW) Category I Auxiliary Gas Supply (FSAR/USAR Section 7.3.6.1.1.h)

NSSS ESFAS support systems: (FSAR/USAR Section 7.3.8.1.1.i)

- Essential Service Water System
- Component Cooling Water System
- Electrical power distribution systems (includes LSELS and EDG Controls)
- Essential HVAC Systems

Engineered Safety Features System (ESFS) Auxiliary support systems: (FSAR/USAR Section 7.3.8.1.1.i and Table 7.3-12)

- Component Cooling Water System
- Essential Service Water System
- Containment Spray System
- Emergency Exhaust System
- Diesel Generator Building Ventilation
- Essential Service Water Pump House Ventilation

- Main Steam System
- Main Feedwater System

The ESFAS and any support system listed above that is part of an ESFAS sense and command path will be assessed for potential common-mode failures along with the previously mentioned RPS. The only ESFAS support system that is part of ESFAS sense and command is the electrical power distribution system, which includes the EDG controls and LSELS.

4.2.2.1 Description of the Current NSSS ESFAS

The NSSS ESFAS consists of the decision logic processing of outputs from the signal processing equipment bistables. To meet the redundancy requirements, two trains of ESF actuation, each performing the same functions, are provided. If one train is taken out of service for maintenance or test purposes, the second train will provide ESF actuation for the unit. If both trains are taken out of service or placed in test, a reactor trip will result. Each train is packaged in its own cabinet for physical and electrical separation to satisfy separation and independence requirements.

The SSPS consists of two parts: the RTS, which is described in Section 4.2.1, and the NSSS ESFAS, which is described here. The ESFAS monitors selected plant parameters and, if predetermined trip setpoints are exceeded, transmits signals to logic matrices sensitive to combinations indicative of primary or secondary system boundary ruptures (Condition III or IV events). When certain logic combinations occur, the system sends actuation signals to the appropriate ESF components.

The equipment which provides the actuation functions is listed below:

- W7300 Process Instrumentation and Control System
- SSPS
- Engineered safety feature test cabinet
- Manual actuation circuits

The NSSS ESFAS consists of two discrete portions of circuitry: an analog portion consisting of three or four redundant channels per parameter or variable to monitor various plant parameters, such as the RCS and steam system pressures, temperatures and flows, and containment pressures; and a digital portion consisting of two redundant logic trains which receive inputs from the analog protection channels and perform the logic needed to actuate the engineered safety features. Each digital train is capable of actuating the ESF equipment required. Any single failure within the ESFAS does not prevent system action, when required.

Each NSSS ESFAS train has a built in testing device that can automatically test the decision logic matrix functions and the actuation devices while the unit is at power. When any one train is taken out of service for testing, the other train is capable of

providing unit monitoring and protection until the testing has been completed. The testing device is semiautomatic to minimize testing time.

The actuation of ESF components is accomplished through master and slave relays. Each master relay energizes one or more slave relays, which then cause actuation of the end devices. The master and slave relays are routinely tested to ensure operation. The test of the master relays energizes the relay, which then operates the contacts and applies a low voltage to the associated slave relays. The low voltage is not sufficient to actuate the slave relays but only demonstrates signal path continuity. The slave relay test actuates the devices if their operation will not interfere with continued unit operation. For the latter case, actual component operation is prevented by the slave relay test circuit, and slave relay contact operation is verified by a continuity check of the circuit containing the slave relay.

4.2.2.2 BOP ESFAS

The BOP ESFAS portion of the system processes signals from the integrated safeguards signal processing equipment (e.g., LSELS), and plant radiation monitors to actuate certain ESF equipment. There are two redundant trains of BOP ESFAS (separation groups 1 and 4), and a third separation group (separation group 2) to actuate the turbine driven AFW pump and reposition automatic valves (turbine steam supply valves, turbine trip and throttle valve) as required. The separation group 2 BOP-ESFAS cabinet is considered to be part of the end device (i.e., the turbine driven AFW pump). The redundant trains provide actuation for the motor driven AFW pumps (and reposition automatic valves as required, i.e., steam generator blowdown and sample line isolation valves, essential service water supply valves, condensate storage tank supply valves), Containment Purge Isolation, Control Room Emergency Ventilation, and Emergency Exhaust Actuation functions.

4.2.2.3 Main Steam and Feedwater Isolation System (MSFIS)

The MSFIS controls the hydraulic actuators for eight actuation valves, four valves control the main steam lines and four the feedwater lines. The MSFIS controls four solenoids in each hydraulic actuator, through four contacts of separate actuation relays, installed in the MSFIS cabinets. Overall, each separation group in its dedicated cabinet contains 32 (4x8) actuation relays.

4.2.3 Description of the Current Load Shedder and Emergency Load Sequencer (LSELS)

The DGs provide a source of emergency power when offsite power is either unavailable or is insufficiently stable to allow safe unit operation. If a loss of voltage condition occurs at the 4.16 kV ESF buses, undervoltage protection provided by the LSELS will perform the following functions.

These functions will be performed in-kind by redundant TXS systems:

- Degraded Voltage Load Shedding: Trip the 4.16 kV preferred normal and alternate bus feeder breakers to remove the deficient power source to protect the Class 1E equipment from damage.

- Undervoltage Load Shedding: Trip the 4.16 kV preferred normal and alternate bus feeder breakers to remove the deficient power source to protect the Class 1E equipment from damage, generate an loss of offsite power (LOP) DG start signal for DG start, and shed all loads from the bus except the Class 1E 480 VAC load centers and centrifugal charging pumps to prepare the buses for re-energization.

- LOCA Load Shedding: Shed all non-safety related loads from the bus to prepare the bus for LOCA sequencing of safety related loads.

- Emergency Load Sequencing: The shutdown load sequencer activates selected loads that are necessary to safely shut down the plant following a loss of offsite power. The LOCA load sequencer actuates selected loads which are necessary to mitigate the effects of a LOCA and safely shut down the plant.

There are two sets of undervoltage protection circuits, one for each 4.16 kV Class 1E system bus. Each set consists of a loss of voltage and degraded voltage function. Four potential transformers on each bus provide the necessary input voltages to the protective devices used to perform these functions. The undervoltage protection circuits are described in FSAR/USAR Section 8.3.1.1.3 (Reference /5/ and /24/).

Four instantaneous undervoltage relays with an associated time delay are provided for each 4.16 kV Class 1E system bus for detecting a loss of bus voltage. The outputs are combined in a two-out-of-four logic to generate an LOP signal if the voltage is below approximately 70% for 1 second (nominal delay). The time delay prevents undesirable trips arising from expected transient undervoltage conditions during large motor starts.

Four degraded voltage bistables with associated time delays are provided for each 4.16 kV Class 1E system bus for detecting a sustained degraded voltage condition. Once the bistable has actuated, a timer in the LSELS circuitry provides an 8 second time delay to avoid false actuation on large motor starts other than an RCP. There are four of these 8-second timers per bus, one for each degraded voltage channel. The bistable outputs are then combined in a two-out-of-four logic to generate a degraded voltage signal if the voltage remains below approximately 90%. Once the two-out-of-four logic is satisfied, contacts in the bus feeder breaker trip circuits close to arm the tripping circuitry. If a safety injection signal (SIS) were to occur concurrently with or after the arming of the tripping circuitry, the bus feeder breaker would open immediately, a bus undervoltage would be sensed, and a LOP signal would be generated. Should the degraded voltage condition occur in a non-accident condition (no SIS present), an additional 111 second

time delay is provided. These time delays are specific to the feeder breakers (2 per bus). If the degraded voltage condition is not alleviated in the overall 119 seconds (nominal delay), the bus feeder breaker is tripped.

4.3 PROPOSED TXS RTS, ESFAS, AND LSELS

The proposed design separates the RTS, NIS inputs, turbine trip inputs, NSSS ESFAS functions, BOP ESFAS functions, MSFIS functions, and LSELS functions into a distributed system. The data acquisition process, the signal validation, the protection logic and the voting for these systems will now be performed by TXS. A block diagram of the proposed RTS, ESFAS, and LSELS is shown in Figure 4-3.

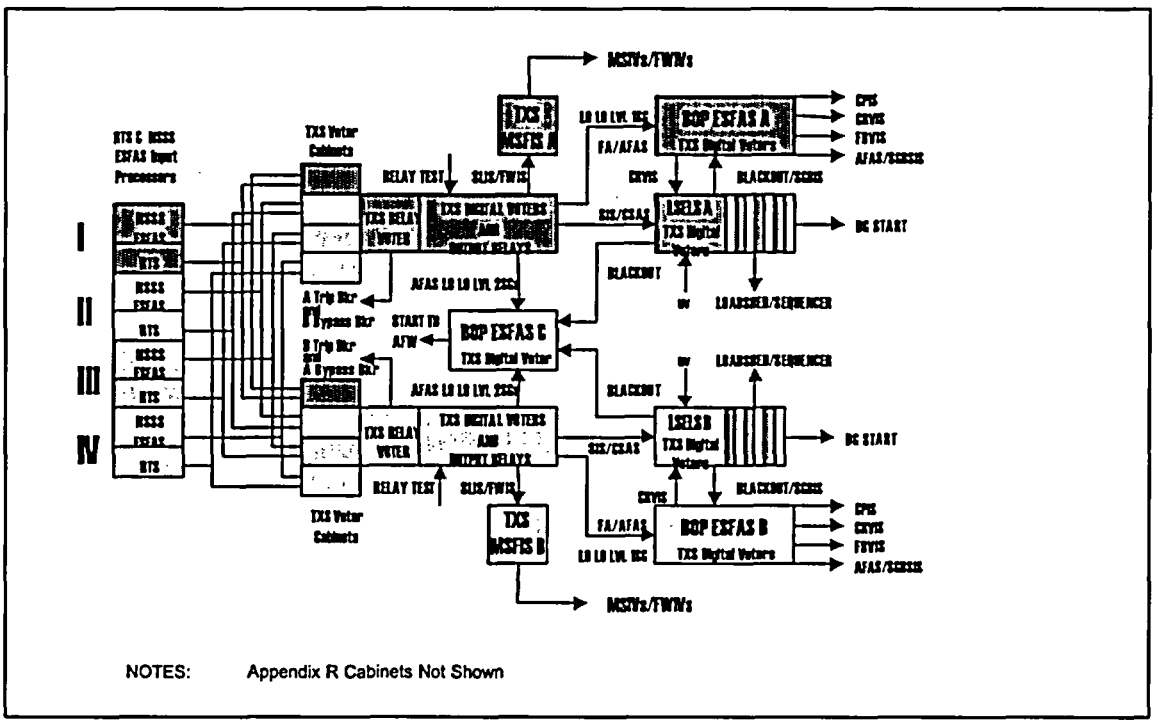


Figure 4-3: Proposed TXS-Based RTS, ESFAS, and LSELS

4.3.1 Proposed Reactor Trip System (RTS) Instrumentation Functions

4.3.1.1 RTS Functions to be Implemented with the TXS System

The TXS system will perform signal conditioning of input signals associated within each protection set group. Control board/main control room/miscellaneous indications will be provided independently of the TXS software. Each protection group will have separate

CPUs to perform RTS functions independently from ESFAS and other safety functions. Shutdown will now be performed by TXS 2/4 actuation voters.

The following RTS functions will performed by the TXS system:

- General warning reactor trip
- Manual reactor trip
- Power range neutron flux high reactor trip
- Power range neutron flux low reactor trip
- Power range high positive neutron flux rate trip
- Intermediate range high neutron flux trip
- Source range high neutron flux trip
- Overtemperature ΔT trip
- Overpower ΔT trip
- Pressurizer low-pressure trip
- Pressurizer high-pressure trip
- Pressurizer high water level trip
- Low reactor coolant flow trip
- RCP undervoltage trip
- RCP underfrequency trip
- SG low-low water level trip
- Low fluid oil pressure turbine trip reactor trip
- Turbine stop valve closure turbine trip reactor trip
- Safety Injection signal reactor trip
- RTS interlocks

Although the manual reactor trip actuation signal will be acquired by TXS, the manual reactor trip actuation will be independently performed by a hardwired connection to the reactor trip breaker, as it is for the current design.

4.3.1.2 NIS Functions to be Implemented with TXS System

The following NIS functions will be incorporated into the TXS system:

- Source range monitoring
- Intermediate range monitoring
- Power range monitoring

The NIS will provide outputs to RTS trip functions.

4.3.1.3 Turbine Trip Functions to be Implemented with TXS System

The following turbine trip functions will be incorporated into the TXS system:

- Main steam turbine stop valve closure
- Main steam turbine control valves hydraulic oil low pressure trips

The turbine trip signals will input directly to RTS trip functions.

4.3.2 Proposed Engineered Safety Features Actuation System (ESFAS) Instrumentation Functions

4.3.2.1 NSSS ESFAS Functions to be Implemented with TXS System

The NSSS ESFAS and remaining SSPS I&C safety functions will be included in the TXS system as follows:

- Safety injection
- Containment spray
- Containment isolation
- Steam line isolation
- Turbine trip and feedwater isolation
- AFW initiation
- Automatic switchover to containment sump
- Automatic pressurizer PORV actuation
- ESFAS interlocks
- Other instrumentation required for safety (all remaining SSPS I&C functions)

Manual system actuations will be independently performed by hardwired connections, as it is for the current design.

4.3.2.2 BOP ESFAS Functions to be Implemented with the TXS System

The BOP ESFAS I&C functions that will be based on the TXS system are as follows:

- Containment purge isolation
- Control Room ventilation isolation
- Fuel Building ventilation isolation
- AFW System actuation
- SG blowdown and sample isolation
- AFW pump suction transfer on pressure low
- AFW System actuation bypass

4.3.2.3 MSFIS Functions to be Implemented with TXS System

- Steam line isolation
- Manual initiation
- Automatic actuation
- Main steam isolation valve (MSIV) Control
- Diverse MSIV Fast Closure
- Feedwater Isolation
- Manual Initiation
- Automatic Actuation
- Feedwater isolation valve (FWIV) Control
- FWIV Isolation Override

Only the test functions of MSFIS will be TXS software-based. Actuation functions will bypass the TXS software using a priority logic module.

4.3.3 Load Shedder and Emergency Load Sequencer Functions to be Implemented with TXS System

The LSELS functions that will be performed by the TXS system are as follows:

- Degraded voltage load shedding
- Undervoltage load shedding
- LOCA load shedding
- Emergency load sequencing

4.3.4 Support Systems and Other Systems Required for Safety to be Implemented with TXS System

4.3.4.1 Emergency Diesel Generator (EDG) Controls

The EDG control functions including control systems for associated systems such as the fuel oil transfer pumps, cooling water and heater will be modernized. It is proposed to install the EDG instrumentation and controls in a standard TXS Voter configuration. The system processes all signals needed for EDG start, EDG trip, and provides analog and binary output signals for EDG auxiliary system status monitoring (analog displays for temperatures and pressures, alarm panel on the EDG cabinet, and alarms to the main control room). Modernization of the EDG instrumentation and controls comprises the following:

- EDG start and shut-down circuits,
- EDG trip circuits with trips based on various monitored pressure and temperature switches (e.g., lube oil, jacket cooling, crank case),
- Annunciators for diesel engine and generator fault conditions,

- Indicators (electrically, or pressure gauges) with associated switches (mainly pressure switches),
- Control of the standby jacket coolant heater and circulation pump, lube oil keep warm heaters and circulation pump, generator space heater and rocker arm pre-lubrication oil pump,
- Thermocouples and resistance temperature detectors (RTDs) for monitoring of exhaust gas, bearing and other temperatures,
- Control of the generator, monitoring of the electric parameters (e.g., voltage, power, frequency) and electric protection,
- Control of the 4.16 kV feeder breaker.

4.3.4.2 Class 1E Analog Controls

Safety I&C functions used for 1E analog controls and monitoring will be replaced by TXS performing the following main functions (only the functions relevant to this assessment have been stated here):

- SGs A to D Main Steam Dump to Atmosphere
- Main Steam Line Loops 1 to 4 Drain Line Drip Pot Levels
- Main Steam Control Valves 1 to 3 Hydraulic Oil Pressure (provides anticipatory turbine trip signal to RTS)
- AFW Flows to SGs A through D
- Auxiliary Feedpump Suction Pressures
- AFW Flow Controls for Flow from Motor Driven Auxiliary Feedpumps to SGs A, B, C and D.
- AFW Flow Controls for Flow from Turbine Driven Auxiliary Feedpump to SGs A, B, C and D.
- AFW Supply Pressure from Condensate Storage Tank
- RCPs A through D Thermal Barrier Cooling Coil Leak Detection Control and Alarm
- Refueling Water Storage Tank (RWST) Temperature Indication and Alarm
- Essential Service Water Pumps Discharge Pressures Indication and Alarm
- Essential Service Water Pumps Discharge Temperature Indication
- Essential Service Water Pumps Pre-Lube Tanks Levels Indication
- Essential Service Water Trains Flows
- Essential Service Water Pumps Strainer Differential Pressure Control, Indication and Alarm
- Essential Service Water Towers A and B Inlet Temperature Control (Callaway Plant only)
- Air Compressors A and B Cooling Water Leak Detection Control
- Component Cooling Water Surge Tank Levels Control, Alarm and Indication
- Component Cooling Water Pumps Discharge Pressure Alarm, Indication and Control
- Component Cooling Water Heat Exchanger Outlet Temperatures Indication and Control

- Component Cooling Water Flow to Non-seismic Piping Control and Indication
- Component Cooling Water Flow to RCS Indication and Alarm
- Component Cooling Water RCP Thermal Barrier Flow Control and Alarm
- Containment Recirculation Sump Levels Indication, Alarm and Recording
- Essential Service Water Pump Room Temperature Control and Indication
- Ultimate Heat Sink Electrical Room Temperature Control and Indication
- Fuel Building Filter ABS Units Charcoal Temperatures Indication and Alarm
- Control Room Filter ABS Units Charcoal Temperature Indication and Alarm
- EDG Building Supply Fan Temperature Control and Indication
- Containment Coolers Inlet Temperature
- Containment H2 Analyzers and Containment H2 Temperatures Indication
- Containment High Range Radiation Monitors Indication
- Emergency Fuel Oil Day Tanks Fuel Levels Control and Indication
- Buildings Sump Levels Indication
- 125 VDC Battery Currents Indication

The above functions will be implemented in their own TXS system, independently from the implementation of other I&C systems. The monitoring will be performed mainly by the OM690, the manual/automatic stations on the main control board (MCB) will be connected to the Control Function Block performed within TXS, however the manual open/close initiation will bypass the TXS software.

4.4 DESCRIPTION OF MONITORING AND INDICATION SYSTEMS

The information about which systems are considered part of Monitoring and Indication Systems is provided in FSAR/USAR Section 7 (Reference /5/ and /24/). Monitoring and Indication Systems are those display instruments which provide information to enable the operator to assess reactor status, the onset and severity of accident conditions, and ESFS status and performance, or to enable the operator to intelligently perform vital manual actions such as safe shutdown and initiation of manual ESFSs. These indications include the information to control and operate the unit through all operating conditions, including anticipated operational occurrences and accident and post-accident conditions. Hot shutdown information is also displayed on the Auxiliary Shutdown Panel (ASP) located outside the main control room. Information about the ASP is provided in FSAR/USAR Section 7.4 (Reference /5/ and /24/).

4.4.1 Reactor Trip System Display Instrumentation

Display instrumentation for the RTS actuation is discussed in FSAR/USAR Sections 7.2 and 7.7 and Tables 7.5-1 and 7.5-2 (Reference /5/ and /24/).

The RTS provides the operator with complete information pertinent to system status and safety. All transmitted signals (e.g., flow, pressure, temperature) which can cause a reactor trip will be either indicated or recorded for every channel, including all neutron

flux power range currents (top detector, bottom detector, algebraic difference, and average of bottom and top detector currents).

Any reactor trip will actuate an alarm and an annunciator. Such protective actions are indicated and identified down to the channel level. Alarms and annunciators are also used to alert the operator of deviations from normal operating conditions so that appropriate corrective action is taken to avoid a reactor trip. Actuation of any rod stop or trip of any reactor trip channel will actuate an alarm.

4.4.2 Engineered Safety Feature System Display Instrumentation

Display instrumentation is provided to monitor actuation parameters, bypasses, status, and performance of the ESFS.

4.4.2.1 System Actuation Parameters

The ESFS actuation parameter display instrumentation comprises of those display instrument channels which will provide for informed operator action during and following an accident. The ESFS actuation parameter displays provide sufficient information to enable the operator to assess accident conditions and to perform the necessary operation of manual ESFS. Each of the ESFS parameters is displayed, providing the operator with information on those parameters indicative of accident conditions. The information supplied by the ESFS actuation parameter displays enables the operator to perform manual actuation.

Containment sump level indication and RWST level indication provide assurance that adequate net positive suction head (NPSH) exists for operation in the sump recirculation mode (FSAR/USAR Chapter 6.0). Main control room ventilation monitors provide the operator with the necessary information on which to base his decision for operation of main control room ventilation isolation and filtration. Containment pressure and air temperature instrumentation provides information for the operator to monitor containment conditions, assess the effectiveness of safety measures in operation, and determine if manual action is necessary. Containment post-accident radiation monitors provide information concerning the radioactive content of the containment atmosphere. Containment hydrogen concentration indication provides information to judge the significance of a metal-water reaction and furnishes the information necessary for manual hydrogen control through the use of the Combustible Gas Control System.

Recording devices provided for the variables furnish trend information, such as the containment pressure and temperature transients, to help predict the course of an accident. In addition, the recording devices provide a historical record for post-accident review.

4.4.2.2 System Bypasses

Bypasses within the ESFS are indicated on the MCB or ESFAS cabinets by lights and are alarmed by the plant computer. Bypass of containment airborne gaseous radiation actuation or of containment purge isolation for periodic testing and maintenance and the bypass of low reactor coolant pressure actuation of the safety injection system for startup and shutdown are examples of such bypasses. Bypass of ESFAS equipment operation can be affected a number of ways. Handswitch in pull-to-lock position, loss of control power, breaker in test or not in operating position, and closure of manual valves for system or device testing or maintenance are some of the means by which an ESFS or vital supporting system might be rendered inoperative on a system level.

The system of status lights for bypass indication, together with other display information available to the operator, and periodic testing provide assurance that the operator will be constantly aware of the status of the ESFS. The automatic indication system assures that bypass of control circuits or manual process valves, which could affect system performance, is immediately made obvious. The bypass indication system is used to supplement administrative procedures by providing indications of safety system availability or status. Administrative procedures will not require operator action based solely on the bypass indicators. The design of the bypass indication system allows testing during normal plant operation. Both indicating and annunciating functions can be verified. Process indicators are provided for ESFS actuation parameters (FSAR/USAR Section 7.5.2.1.1) so that, for parameters that vary in value during plant operation, closure of a manual valve in the transmitter sensing line results in a discrepant indication and response when compared with the corresponding indicators for the redundant channels of the same parameter. The process indicators thus provide indication of impulse line blockage or bypass, which obviates the need for position indication for the manual instrument valves.

For ESFS actuation parameters which do not vary during operation, sufficient redundancy is provided so that more than one manual instrument valve would have to be placed in the wrong position before system level actuation could be blocked. Diversity in actuating parameters and the capability for manual system actuation make it even more improbable that ESFS function can be blocked by improper instrument valve position. For the preceding reasons, instrument valves are not included in the status light displays.

On items that do not affect the ESFS function no indication system is provided for manual valve position or circuit bypass features. Operation of manual valves, use of manual disconnects, or other operations occurring once a year or less frequently, which could impair ESFS performance, are controlled by administrative procedures. Thus, the probability for system blocks or bypasses existing undisclosed between periodic functional tests is minimal.

4.4.2.3 System Status

The information important in evaluating the readiness of the ESFS prior to operation and the status of active components during system operation is displayed for the operator in the main control room. The display information consists of process indicators, indicating lights, alarms, and recorders. The display is sufficient but supplemented by the plant computer outputs.

Indications are provided for levels, pressures, and temperatures important to safety feature operation. Each of the indications is driven by an electronic instrument loop consisting of a transmitter, power supply, and any necessary signal conditioners. Where an alarm is provided, the instrument loop includes an alarm unit providing a contact output to the plant annunciator. Many of the analog signals are monitored by the plant computer to enable CRT display or logging of status or alarm information. Recording devices are provided in lieu of, or in addition to, the indications where a trend or a time history of the process variable is desired. Indicating lights are provided to monitor equipment status. In addition to the system level availability and bypass indicating lights, indicating lights are provided at each control switch for equipment.

Each motor-driven component (e.g., pump, fan) has ON and OFF indicating lights, each remotely controlled open-closed service valve or damper has corresponding OPEN-CLOSED light indication, and each breaker control switch has its associated open-closed indicating light. A red light is used to indicate an operating status; for example, motor running, valve fully open, or breaker closed. The green light indicates that the equipment is not in an operating state; for example, motor off, valve fully closed, or breaker open. Amber lights, where provided, signify equipment bypassed, locked out, or not in automatic readiness. The indicating lights for a given control circuit are operated from the control circuit power. Thus, loss of control circuit power would be accompanied by a loss of indicating lights for that device.

RTDs and thermocouples are utilized to monitor temperatures of tanks subject to a freezing environment or tanks containing boric acid solutions to preclude undisclosed freezing or crystallization and loss of availability.

4.4.2.4 System Performance

Display information important in evaluating the performance of an ESFS during periodic testing, continuous normal operation, or post-accident operation is provided on the MCB. Sufficient process indicators, alarms, and recording devices are provided to enable the operator to determine whether a system is performing normally or if there is some unanticipated failure within a system. The plant computer monitors selected instrument channels to supplement the display information.

For fluid systems, discharge pressure indication is provided for each pump, and flow indication is provided for each system. Together, the flow and pressure enable the operator to verify proper pump performance and verify fluid delivery performance.

Temperature indication is provided for each system heat exchanger inlet and outlet. The operator has the information, together with the system flow, to verify proper cooling performance. Temperature indication is also provided for each ventilation system incorporating charcoal filtration, to verify proper temperature range for expected filter performance. Hydrogen recombiner outlet temperature provides a measure of recombiner performance.

4.4.3 Safe Shutdown Instrumentation

The important display information provided for operator use during safe shutdown operations is described as follows:

4.4.3.1 Hot Shutdown Information Display Systems

The hot shutdown information display systems are designed to protection systems standards, thus the display parameters remain available in the event of a single failure. Redundant indication channels are powered by redundant, 120-V vital instrument ac power supplies (FSAR/USAR Section 8.3.1.1.5). The indication channels are designed in accordance with the portions of IEEE Standard 279-1971 applicable to indication channels. FSAR/USAR Table 7.1-2 identifies the applicable guides and standards for this equipment. Compliance with the design criteria ensures the availability of the display instruments to present the information required to maintain the plant in a hot shutdown condition.

Three channels of narrow range level and pressure are indicated on the MCB for each SG, which enable the operator to control AFW to the SG and to regulate atmospheric relief. Three channels of primary system wide range pressure and pressurizer level are provided which enable the operator to control the pressurizer heaters and coolant inventory. Similar provisions are made on the ASP where one channel of pressure and narrow range level is displayed for each SG and two channels of primary system wide range pressure and pressurizer level are indicated.

4.4.3.2 Cold Shutdown Control

The display instruments required to bring the plant to a cold shutdown condition are provided in the main control room. Instrumentation for cold shutdown from outside of the main control room is listed in FSAR Section 7.4.2/USAR Section 7.4.3.,FSAR/USAR Table 7.5-2, lists the display information provided for cold shutdown control, together with the type of readout, number of channels, and their range, accuracy, and location. Cold shutdown displays and indications will be retained or replaced in kind with equivalent displays and indications. The TXS system provides signals to cold shutdown displays and indication independent of the TXS software.

4.5 THERMOCOUPLE/CORE COOLING MONITOR (TC/CCM) AND REACTOR VESSEL LEVEL INDICATING SYSTEM (RVLIS)

TXS will also perform the acquisition of the safety and PAMS Regulatory Guide 1.97 Category 1 related parameters of the TC/CCM and RVLIS and provide its indication by using a Qualified Display System.

4.5.1 RVLIS

Reactor vessel water level is a Category 1 variable provided for verification and long term surveillance of core cooling. It is also used for accident diagnosis and to determine reactor coolant inventory adequacy.

The RVLIS provides an indication of reactor vessel level from the bottom of the reactor vessel to the top of the reactor during natural circulation conditions and for any combination of operating RCPs.

4.5.2 TC/CCM

The TC/CCM combines the functions of monitoring for excessive core exit thermocouple temperatures and monitoring both core exit thermocouple temperatures and hot and cold leg RTD temperatures for saturation margin.

- RCS Hot and Cold Leg Temperatures (Wide Range):

  RCS hot and cold leg temperatures (Wide Range) are Type A, Category 1 variables provided for verification of core cooling and long term surveillance.

  RCS hot and cold leg temperatures provide input to the core subcooling monitor or may be used to manually determine RCS subcooling margin. RCS subcooling margin is used to determine whether to terminate safety injection (SI), if still in progress, or reinitiate SI if it has been stopped. RCS subcooling margin is also used for unit stabilization and cooldown control.

  In addition, RCS cold leg temperature is used in conjunction with RCS hot leg temperature to verify the unit conditions necessary to establish natural circulation in the RCS.

  Each of the four hot legs and each of the four cold legs has one wide range, thermowell-mounted RTD. These are separate from the narrow range RTDs providing inputs to the RPS. The wide range channels provide indication over a range of 0°F to 700°F. Loops 1 and 2 have hot and cold leg wide range Class 1E temperature indications in the main control room.

- Core Exit Temperature

Core exit temperature is a Category 1 variable which provides for verification and long term surveillance of core cooling.

An evaluation was made in support of References /5/ and /24/ regarding the minimum number of valid core exit thermocouples (CETs) necessary for measuring core cooling. The evaluation determined the reduced complement of CETs necessary to detect initial core recovery and trend the ensuing core heatup. The evaluations account for core non-uniformities, including incore effects of the radial decay power distribution, excore effects of condensate runback in the hot legs, and non-uniform inlet temperatures. Based on these evaluations, adequate core cooling is ensured with two valid core exit temperature channels per quadrant with two CETs per required channel. Core exit temperature is used to determine whether to terminate SI, if still in progress, or to reinitiate SI if it has been stopped. Core exit temperature is also used for unit stabilization and cooldown control.

Two operable channels of core exit temperature are required in each quadrant to provide indication of radial distribution of the coolant temperature rise across representative regions of the core.

Variables for the new TXS TC/CCM and RVLIS will be displayed on the Qualified Display System described in the following section.

4.6 PAMS INSTRUMENTATION - QUALIFIED DISPLAY SYSTEM

The primary purpose of the Qualified Display System (Safety and Diverse Indication and Control Panel) is to display unit variables for the new TXS TC/CCM and RVLIS as well as the current PAMS. These systems provide accident monitoring instrumentation required by the main control room operators during accident situations. This information provided by the Qualified Display System provides the necessary support for the operator to take the manual actions for which no automatic control is provided and that are required for safety systems to accomplish their safety functions for Design Basis Accidents (DBAs).

The accident monitoring instrumentation consists of 2 Qualified Display Systems per train with sufficient information available on selected unit parameters to monitor and to assess unit status and behavior following an accident. One Qualified Display System in each train is dedicated as a continuous display. The availability of accident monitoring instrumentation is important so that responses to corrective actions can be observed and the need for, and magnitude of, further actions can be determined.

The instrument channels required include two classes of parameters identified during unit specific implementation of Regulatory Guide 1.97 as Type A variables or

non-Type A, Category 1 variables that meet Criterion 4 of 10CFR50.36(c)(2)(ii). Type A variables are included because they provide the primary information required for the main control room operator to take specific manually controlled actions for which no automatic control is provided, and that are required for safety systems to accomplish their safety functions for DBAs. Selected Non-Type A instrumentation is included to assist operators in minimizing the consequences of accidents.

Regulatory Guide 1.97 Type A and required non-Type A Category 1 variables ensure the main control room operating staff can perform the diagnosis specified in the emergency operating procedures (these variables are restricted to preplanned actions for the primary success path of DBAs), e.g., LOCA.

Regulatory Guide 1.97 Type A variables provide information necessary to:

- Take the specified, pre-planned, manually controlled actions, for which no automatic control is provided, and that are required for safety systems to accomplish their safety function;
- Determine whether systems important to safety are performing their intended functions;
- Determine the likelihood of a gross breach of the barriers to radioactivity release;
- Determine if a gross breach of a barrier has occurred; and
- Initiate action necessary to protect the public and to estimate the magnitude of any impending threat.

Regulatory Guide1.97 Type A variables include:

- RCS Hot Leg Temperature (Wide Range)
- RCS Cold Leg Temperature (Wide Range)
- RCS Pressure (Wide Range)
- Containment Normal Sump Water Level
- Containment Pressure (Normal Range)
- Steam Line Pressure
- Containment Radiation Level (High Range)
- Pressurizer Water Level
- SG Water Level (Narrow Range)
- RWST Level

Category 1, non-Type A variables provide information important for reducing public risk. Non-Type A Category 1 variables are deemed risk significant because they are needed to:

- Determine whether other systems important to safety are performing their intended functions;

- Provide information to the operators that will enable them to determine the likelihood of a gross breach of the barriers to radioactivity release; and

- Provide information regarding the potential release of radioactive materials to allow for early indication of the need to initiate action necessary to protect the public, and to estimate the magnitude of any impending threat.

The required non-Type A, Category 1 variables include:

- Neutron Flux
- RVLIS
- SG Water Level (Wide Range)
- Containment Hydrogen Concentration Level
- Core Exit Temperature

In addition, AFW Flow Rate is a required non-Type A, Category 2 variable. These variables are considered essential to the operator for accident management.

4.7 DESCRIPTION OF CURRENT CONTROL SYSTEMS

The information about which systems are considered part of control systems is provided in the FSAR/USAR Section 7.7 (Reference 5/24). The control systems are those systems that exercise normal control of the reactor and to maintain the reactor within normal operating parameters. The general design objectives of the control systems are:

- To establish and maintain power equilibrium between the primary and secondary system during steady state unit operation.
- To constrain operational transients so as to preclude unit trip and reestablish steady state unit operation.
- To provide the reactor operator with monitoring instrumentation that indicates all required input and output control parameters of the systems and provides the operator with the capability of assuming manual control of the system.

The control systems perform the following functions:

4.7.1 Reactor Control System

Callaway Plant

The Reactor Control System enables the nuclear plant to accept a step load decrease of 10 percent and a ramp decrease of 5 percent per minute over the entire power range without reactor trip, steam dump, or pressurizer relief actuation, subject to possible

xenon limitations. It maintains reactor coolant average temperature (T_{avg}) within prescribed limits by creating the bank demand signals for manually moving groups of rod cluster control assemblies during normal operation and operational transients. The T_{avg} control also supplies a signal to pressurizer water level control and steam dump control.

WCGS

The Reactor Control System enables the nuclear plant to accept a step load increase or decrease of 10 percent and a ramp increase or decrease of 5 percent per minute within the load range of 15 percent to 100 percent without reactor trip, steam dump, or pressurizer relief actuation, subject to possible xenon limitations. It maintains reactor coolant average temperature T_{avg}) within prescribed limits by creating the bank demand signals for moving groups of rod cluster control assemblies during normal operation and operational transients. The T_{avg} control also supplies a signal to pressurizer water level control and steam dump control.

4.7.2 Rod Control System

The Control Rod System provides for reactor power modulation by manual or automatic (insertion only for the Callaway Plant) control of control rod banks in a preselected sequence and for manual operation of individual banks. It also provides monitoring and indication that provide alarms that alert the operator if the required core reactivity shutdown margin is not available due to excessive control rod insertion, to display control rod position, and to provide alarms to alert the operator in the event of control rod deviation exceeding a preset limit.

4.7.3 Control System Interlocks

Control System interlocks prevent further withdrawal (manual only for the Callaway Plant) of the control banks when signal limits are approached that indicate the approach to a DNBR limit or kW/ft limit and limit automatic turbine load increase to values for which the NSSS has been designed.

4.7.4 Pressurizer Pressure Control

Pressurizer pressure control maintains or restores the pressurizer pressure to the design pressure ±35 psi (which is within reactor trip and relief and safety valve actuation setpoint limits) following normal operational transients that induce pressure changes by control (manual or automatic) of heaters and spray in the pressurizer. It provides steam relief by controlling the power relief valves.

4.7.5 Pressurizer Water Level Control

Pressurizer water level control establishes and maintains the pressurizer water level within specified limits as a function of the average coolant temperature. Changes in level are caused by coolant density changes induced by loading, operational, and

unloading transients. Level changes are produced by means of charging flow control (manual or automatic) as well as by manual selection of letdown orifices. Maintaining coolant level in the pressurizer within prescribed limits by actuating the charging and letdown system provides control of the reactor coolant water inventory.

4.7.6 Steam Generator Water Level Control

Establishes and maintains the SG water level within predetermined limits during normal operating transients. The SG water level control system also maintains the SG water level to within predetermined limits and unit trip conditions. It regulates the feedwater flow rate so that under operational transients the water level for the SG does not decrease below a minimum value. Steam generator water inventory control is manual or automatic through the use of feedwater control valves.

4.7.7 Steam Dump Control (Turbine Bypass)

Permits the nuclear plant to accept a sudden loss of load without incurring reactor trip. Steam is dumped to the condenser and/or the atmosphere, as necessary, to accommodate excess power generation in the reactor during turbine load reduction transients. Ensures that stored energy and residual heat are removed following a reactor trip to bring the plant to equilibrium no-load conditions without actuation of the SG safety valves. Maintains the plant at no-load conditions and permits manually controlled cooldown of the plant.

4.7.8 Incore Instrumentation

Provides information on the neutron flux distribution and on the core outlet temperatures at selected core locations.

4.7.9 ATWS Mitigation System Actuation Circuitry (AMSAC)

AMSAC automatically initiates AFW and a turbine trip under conditions indicative of an ATWS event. AMSAC actuation ensures that RCS pressure will remain below the ASME B&PV Code Level C service limit stress criteria (3200 psig) after the most severe ATWS events (loss of external electrical load or loss of normal feedwater flow), per WCAP-8330 (Reference /25/) and Reference /3/.

4.8 DESCRIPTION OF PROPOSED CONTROL SYSTEMS: TXP PROCESS INFORMATION AND CONTROL SYSTEM OM690 AND PROCESS AUTOMATION SYSTEM

The following control systems will be TXP-based and are independent and diverse from the TXS systems:

1. Reactor Control System
2. Rod Control System
3. Control System Interlocks
4. Pressurizer Pressure Control
5. Pressurizer Water Level Control
6. Steam Generator Water Level Control
7. Steam Dump Control
8. Incore Instrumentation
9. AMSAC

TXP is the automation system for any other application in power plant control. TXP consists of:

- Automation processors (AP) performing automation functions like binary logic control, sequence control or closed loop control.
- Function Modules (FUM) respectively Signal Modules (SIM), dealing with signal acquisition and signal output.
- Operating and Monitoring system (OM), which consist of a set of Processing Units (PU) performing man-machine interface-related signal processing and short-term data logging. The OM is supported by a Server Unit (SU) for data storage, and a set of Operator Terminals (OT), performing all the functions linked to Human Machine Interface (HMI)-dialogues via CRTs and large screens. Any screen is capable of performing any HMI-function (presentation of alarms, information display, and manual control); however, functions may be restricted according to the right of the operator logged in. Communication between PUs and OTs is performed by a separate terminal bus.

Specific application functions, such as nuclear calculations, are performed using separate processing units such as PU-Core.

4.9 NEW COMPONENTS AND INTERFACES

In addition to the Qualified Display System, Figure 4-1 shows an interface to three new components not currently used at the Callaway Plant and WCGS: AV42 Priority Control Modules, Monitoring and Service Interfaces and Gateways.

4.9.1 AV42 Priority Control Module

[

]

4.9.2 Function of the Monitoring and Service Interface

The Monitoring and Service Interface (MSI) consists of the same CPU and communication capabilities as the TXS application processors. As such, they are programmed in the same manner as the application processors. They perform monitoring and reporting of system status and relay messages containing this data between the application processors and the non-Class 1E portions of the system, e.g., the Service Unit and gateway computer. The function of the MSI has no direct equivalent in the existing I&C systems. However, the MSI plays an important role for every complex TXS system in providing a barrier between the Class 1E safety function applications and the corresponding surveillance system.

[

]

4.9.3 TXS-TXP Gateway

The TXS-TXP Gateway is a programmable computer used for isolation between safety related and non-safety related systems. The TXS-TXP Gateway retrieves numeric process data and binary status information from the TXS and sends it to OMs of the TXP system on a continuous basis. The TXS-TXP Gateway is programmed to only allow data to flow in an outward direction. No outside systems are allowed to have communication or cause interrupts with the safety related system.

5 TXS SYSTEM ARCHITECTURE AND SYSTEM DIVERSITY

The purpose of this section is to describe the design architecture and diverse system features built into the TXS system to prevent a software common-mode failure. The TXS systems use special architecture and features to incorporate both hardware and software diversity necessary to prevent the occurrence of common-mode failures. Special emphasis is placed on RTS and ESFAS designs and the prevention of software common-mode failures. The below listed design features 2 to 10 are extended to the other TXS systems, which results in all TXS systems having high levels of diversity, reduced failure modes, high reliability and high availability. Diverse features used in the TXS system include but are not limited to: [

6. TXS Voters and Master/Checker CPUs: Voting of actuation signals will now use inputs from all protections sets. Checking by master/checker voter pairs of CPUs provide an additional level of redundancy.
7. On-line signal validation: Signal validation is used to eliminate questionable or faulted input data.
8. Watchdog Monitoring: Independent watchdog circuitry ensures outputs de-energize to predefined fail-safe states when the CPU exceeds acceptable application program or self-monitoring program cycle times.
9. Independent Indication, Monitoring, and Manual Controls: Provisions for software indications, monitoring, and manual controls independent of TXS software.
10. Diverse Plant Information and Controls Systems: Provisions for signals, independent of the TXS software, to diverse Plant Information and control system functions and ATWS functions performed by other diverse systems (e. g., TXP).

Each of the above diverse design features is carefully selected and applied to RTS and ESFAS as well as other TXS systems. The design is then apportioned into system blocks and analyzed for common-mode failure. After analyzing the vulnerabilities of the TXS design to a common-mode failure, the assessment then qualitatively reevaluates the response to all of the applicable FSAR/USAR Chapter 15 transients and accidents

as well as additional selected transients and accidents that include Containment Functional Design, High Energy Line Break (HELB), and Main Steam Line Break (MSLB) outside the containment. The report subsequently documents how the assessment of FANP, AmerenUE, and WCONOC concepts to address D-in-D&D compared against the NRC guidance and acceptance criteria in BTP HICB-19 using the above design assumptions. The results of the evaluation are presented in Section 8 of this report.

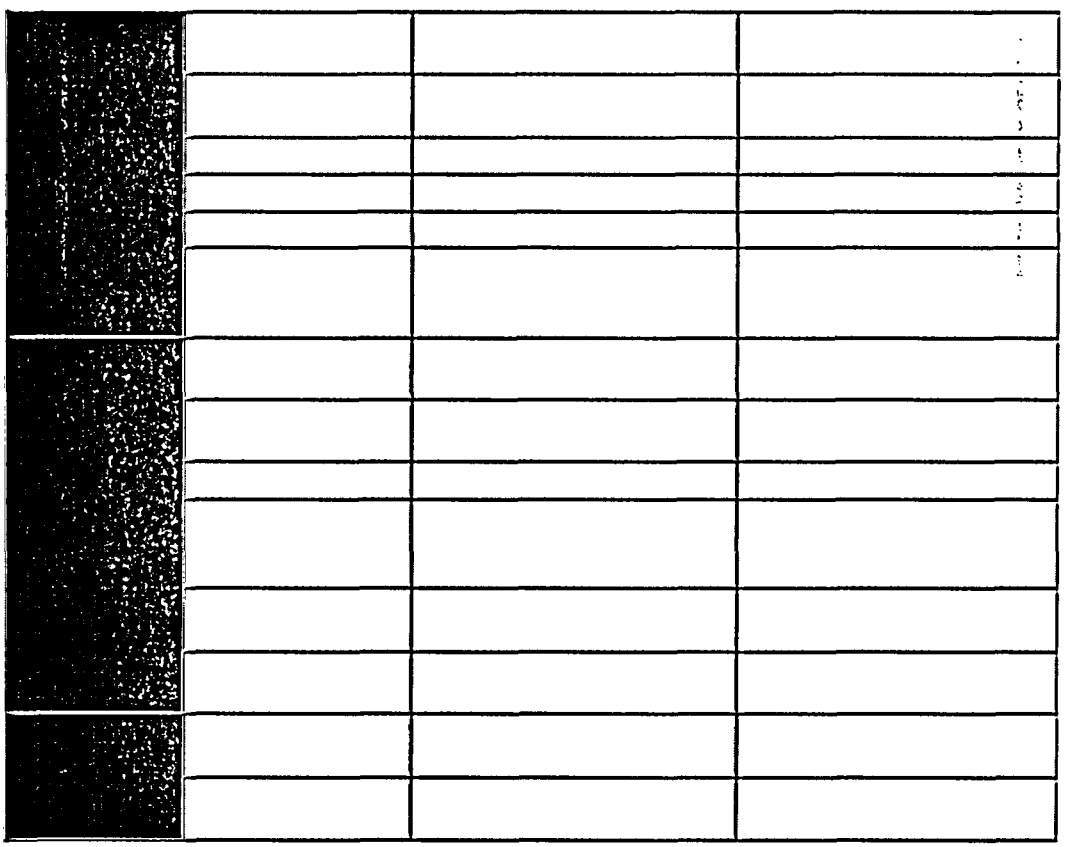
The purpose of examining software blocks within the TXS system is to configure blocks so that a failure cannot propagate to the outside or spread to independent blocks and so that failures cannot propagate inside. The assumption was made that the postulated failures within a block cause the most detrimental credible output signal and the entire block fails and that all of its output signals assume detrimental values. It was assumed that all identical blocks fail concurrently including across divisions and this assumption was repeated until the list of diverse blocks was exhausted. The blocks were assumed to be identical if the likelihood of common-mode failure affecting two or more blocks is not acceptably low.

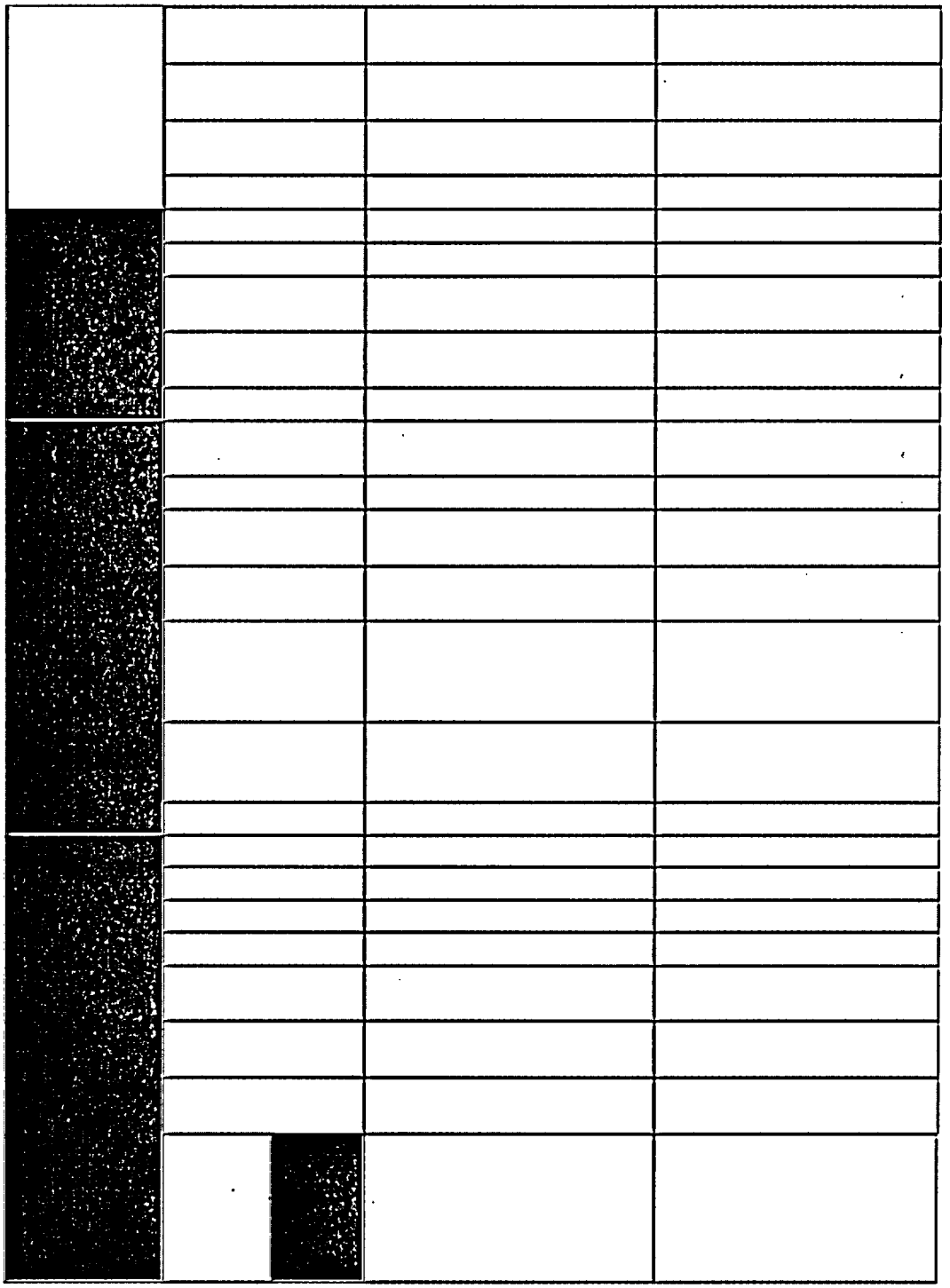
[

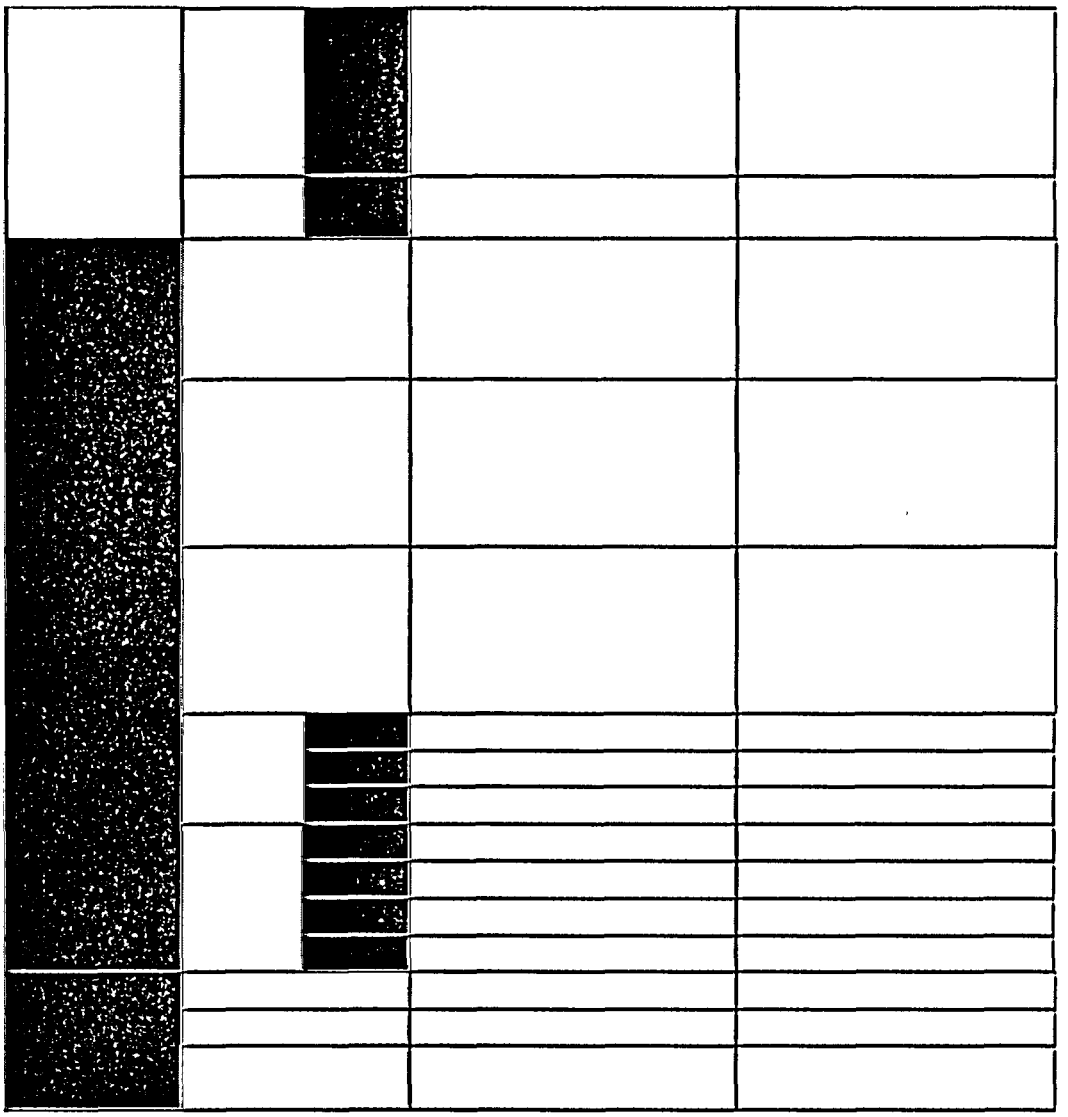
]

5.1 FUNCTIONAL SEPARATION AND INDEPENDENCE

The input signals for the TXS Acquisition Units are grouped exactly like in the existing Process Protection Sets with the exception that NIS trip and turbine trip signals, which will now be input directly as RTS inputs. [







]

5.4 ASYNCHRONOUS OPERATION

The timing of a distributed TXS system is determined by the following fundamental system features:
[

]

5.5.3 Application Software

The application software is designed using the advanced SPACE engineering system. To minimize the probability of design errors, the design notation for the intended application functions is prepared in the proven format of function diagrams. Function diagrams are easy to understand for I&C engineers and system designers. The I&C system architecture is also designed using the SPACE engineering system. As such, the building of applications requires no programming by the I&C engineer; the engineer simply assembles the application using pre-qualified and tested function blocks.

Advanced automatic checks are integrated in the SPACE engineering system in order to detect errors in input data. It also allows the engineer to design processor and busloads by optimizing the architecture (e.g. by parallel processing), and to allocate functionality to different processors within the I&C system. These checks also include the prediction of the overall response time. The documentation of the I&C system specification, which is stored in the design data bank, is reviewed against the basic requirements specification.

The database created by the above process is compiled into the processor code and by virtue of diverse processor operation described above results in diverse software execution.

5.5.4 Cyclic Processing of the Application Function

The application function implemented on each CPU is processed strictly cyclically and is characterized by the following tasks:
[

]

5.5.5 Code Generation, Compilation

5.5.5.1 Overview

The complete TXS application software design process is handled by the TXS engineering tool set SPACE. The application code is automatically generated by the TXS code generators FDGM and RTE based on design information stored in the TXS engineering database. The application code is compiled and, afterwards, linked to the system software components. The final executable code is located to static memory addresses Identifiers in the SPACE data model assigned during the design.

The SPACE data model used in the TXS engineering database uses internal ID numbers to identify the design elements, which are implemented by using the graphical user interface – the function diagram editor FDE.
[

]

5.5.5.2 Identifiers in the SPACE Data Model Assigned During Code Generation

The code generators analyze the design stored in the engineering database and assign additional IDs:
[

]

5.5.6 Sequencing

It is the task of the code generators to translate a "two dimensional" design of function diagrams and hardware diagrams into an "one dimensional" sequence of cyclic code execution as described in Section 5.5.4

5.5.6.1 Sequence of I/O Driver Calls

The sequence of I/O driver calls is defined by the local ID of the respective I/O board symbol on the hardware diagram. [

]

5.5.6.2 Structure of the I/O Driver Data Structure

The data read by the I/O drivers from a single I/O board is stored in the I/O driver data structure on a channel-by-channel basis.

[

]

5.5.6.4 Structure of the FDG Message Data Structure

The data read by the communication drivers for a single FDG message is stored in the FDG message data structure in a sequence defined by the code generators. [

]

5.5.6.5 Sequence of Calling Function Diagrams

The sequence of calling FDs within a FDG is defined by the code generators. [

]

5.5.6.6 Sequence of Calling Function Blocks Inside Function Diagrams

The sequence of calling FBs within a FD is defined by the code generators. [

]

5.5.6.7 Sequence and Structure of the Output Data

The sequence of calling the output I/O drivers and the structure of the I/O data is similar to the inputs as described above.

The sequence of calling the output communication drivers and the structure of the output FDG message data is similar to the inputs as described above.

5.5.6.8 Summary – Application Software

Because of the data model and the design and code generation methods, the code designed and generated on redundant computers is not identical by default. [

]

5.5.7 Operating Software and Runtime Executive

By using the guidance of NUREG/CR-6303, the likelihood of a software common-mode failure to the operating software is reduced to an acceptable level by several TXS design features. As per NUREG/CR-6303, the assumption has been made that the operating software programming is such that software failures are related to service demands and that service demands are distributed differently enough in the dissimilar chosen blocks (i.e. RTS, NSSS ESFAS, BOP ESFAS, LSELS, and EDG controls) to exclude the operating system as a separate cause of common-mode failure. The validity of this type of assumption is discussed in the NUREG, where it is stated that this is not valid if the operating system is complex or multitasking or where more than a simple clock-updating timer is used. [

]

5.6 VOTERS AND MASTER/CHECKER CPUS

5.6.1 Reactor Trip 2/4 Actuation Voter

The TXS 2/4 actuation voter votes the four redundant trip signals, one from each TXS channel set, with a simple 2-out-of-4 logic. The relays are duplicated for Train A and Train B (Figure 5.8, "2/4 Actuation Voter for Reactor Trip (Train A or B)"). Each combination of the 2/4 logic is testable. The TXS monitoring and service interface is used for test and monitoring purposes.
[

5.6.2 TXS Digital Actuation Voters with Master/Checker Pair for ESFAS

All of the ESFAS, LSELS and all other Class 1E analog control actuations are comprised of actuation voters (Figure 5-9, "TXS Digital Voter"). The reactor trip signals are voted by highly reliable 2/4 actuation voters, and the ESF actuation signals by the TXS digital voters. [

5.7 ON-LINE SIGNAL VALIDATION

Data comparison (data validation) between redundant values is performed to select trustworthy values and to prevent faults from data errors through the following techniques:

- Range checks are performed.
- Consistency checks between values are performed.
- Signals that are outside of the specified signal deviation, out of range, or in test are taken out of the value selection.
- Faulted values are announced to the operator.

5.7.1 The On-Line Analog Signal Validation Process

Analog signal processing consists of signal distribution, monitoring, validation and announcing:

[

]

5.7.2 Binary Signal Monitoring

The input signals for the reactor trip logic are negative logic; this means they are normally energized and de-energize to trip. So the fault of an input signal will be recognized with a partial trip actuation.

[

]

5.8 WATCHDOG MONITORING

TXS processing modules (CPU boards) feature a hardware watchdog, which is implemented in the System Support Controller (SSC) and is controlled by a clock that is independent from the CPU clock. [

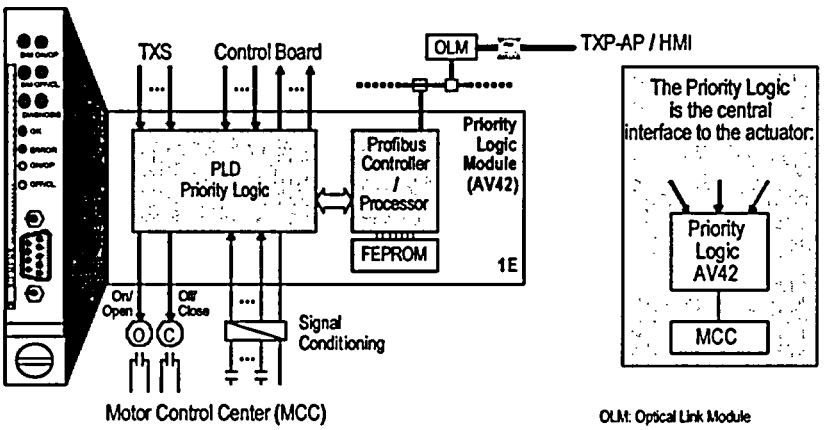
]

5.9 INDEPENDENT INDICATORS, MONITORING, AND MANUAL CONTROLS

The signal conditioning is implemented in the four redundant channel sets. Figure 5-12, "SAA1 Analog Signal Module" shows the structure and functions of the analog signal conditioning, as well as the related data acquisition by TXS input modules, in one channel set.

[

ESF Output Configuration. Example with Priority Logic



]

For the TC/CCM, RVLIS and PAMS indication, a Qualified Display System will be used to present required Regulatory Guide 1.97 variables (Reference 28). This system will consist of environmentally qualified PC based equipment with LCD flat panel displays and a safety class multi-task operating software and graphical library to develop the necessary screens. [

]

5.10 DIVERSE PLANT INFORMATION AND CONTROL SYSTEM

In the defense-in-depth concept of the plant, the control systems, RTS, ESFAS, and Monitoring and Indication Systems represent the main line of defense. A second line of defense is provided by a combination of control systems, AMSAC, and manual controls. In the very unlikely event the RPS is unavailable due to two different postulated software common-mode failures, the FANP architecture has been carefully designed to assure that the control systems, AMSAC, and indications necessary for operator action remain available. It is important to note that the isolated output signals to the NSSS control systems are also not affected by the unlikely event of a postulated software common-mode failure in the TXS Protection System. Most of the non-safety related I&C systems will be upgraded with the diverse TXP system, which receive hardwired interconnections from the output of these signal-conditioning modules and, as a result, remain independent and diverse from the TXS system. (TXP diversity is discussed in Section 7 of this report.) In addition the TXP upgrade to the AMSAC assures that this system remains a diverse and independent system that continues to meet the ATWS Rule.

[

]

5.11 SOFTWARE DIVERSITY BETWEEN OTHER TXS SAFETY SYSTEMS

All TXS systems can be considered diverse from each other. [

] By using the guidance contained in NUREG/CR-6303 (*APPENDIX-BLOCK EXAMPLES*), the case can be made that the software based RPS functions and the other TXS safety functions processed by the TXS system are both diverse and independent from each other. [

]

The NUREG also states that the standard for independence between the systems (i.e., RPS, EDG controls and LSELS) is that they must differ significantly in parameters, dynamics, and logic. Neither the EDG controls nor the LSELS contain similar actuation logic to the RTS or ESFAS. The same is true for other TXS safety systems shown in Figure 4-1. [

]

6 SYSTEM DEPENDABILITY

The TXS system employs several diverse techniques/aspects that prevents the occurrence of a software common-mode failure by maximizing TXS dependability.

Quality and D-in-D&D are all necessary characteristics that have to meet/follow certain standards for safety related software. The TXS software is of the highest quality and has been accepted by the NRC for use in safety related systems (NRC safety evaluation dated May 5, 2000 (Reference /11/)). Quality features of the TXS software are discussed in many FANP documents, including EMF-2267 (Reference /6/) and EMF 2110 (Reference /2/) and within the NRC safety evaluation (Reference 29). The TXS software was designed using the guidance provided in IEC 880 (Reference /12/), the supplement to IEC 880 (Reference /13/), and Regulatory Guide 1.152 (Reference /14/).

6.1 DETERMINISTIC SYSTEM BEHAVIOR

The TXS system is designed to exhibit deterministic I&C system behavior. This means that the overall system behavior in response to any input data trajectories is determined by the validated application software and is free of any unintended interference from the operating system software or the system hardware.

The hardware modules are designed and qualified by tests to perform their intended functions under environmental stress. This ensures that system failures caused by environmental effects can be prevented while operating within the design requirements of the relevant I&C safety system standards.

To ensure that the system's operating behavior is independent from any input data trajectories, the following set of system features is implemented:

- Strict cyclic system operation.
- No process-dependent interrupts.
- Static allocation of system resources.
- Interference-free communication between subsystems as fault barrier so that single failures in one train cannot propagate to redundant systems.

To ensure highest quality, the complete development process documentation set underwent a high integrity qualification process, which was performed by independent experts. The function block modules are developed and qualified in the same way according to the requirements of IEC 880.

All of the system specifications were confirmed during generic tests on a redundant four-train system, performed in the presence of independent experts from GRS-ISTec and TÜV-Nord. The confirmed deterministic system behavior is the essential precondition for

ensuring that, for an individual I&C system, the final behavior of the integrated system corresponds to its design specification.

Deterministic control of common-mode failure of a safety system implemented with TXS demands that a number of design requirements are met:

- Redundant equipment is tested periodically at staggered intervals so that the relative operating time of the automation computer differs sufficiently between the separate trains.
- The cycle for the periodic testing must be set such that no dangerous accumulation of hidden failures in digital I/O modules can arise even in the event of a significant rise in failure rates.

With these design requirements implemented, the safety function performs as intended even in the presence of any plausible production errors or manufacturing defects.

6.2 QUALITY OF DESIGN PROCESS

The TXS quality design process focuses on ensuring that the functional requirements for the nuclear power plant application are fulfilled by the application software.

6.2.1 Automated Tools

The application software is designed using the advanced SPACE engineering system. To minimize the probability of design errors, the design notation for the intended application functions is prepared in the proven format of function diagrams. Function diagrams are easy for I&C engineers and system designers to understand. The I&C system architecture is also designed using the SPACE engineering system.

Figure 6-1, "Quality of the TXS Engineering Process," displays the straightforward engineering process for designing I&C systems in conjunction with the verification and validation phases. Advanced automatic checks are integrated in the SPACE engineering system in order to detect errors in input data. It also allows the engineer to design processor and busloads by optimizing the architecture (e.g., by parallel processing), and to allocate functionality to different processors within the I&C system. These checks also include the prediction of the overall response time. The documentation of the I&C system specification, which is stored in the design database, is reviewed against the basic requirements specification.

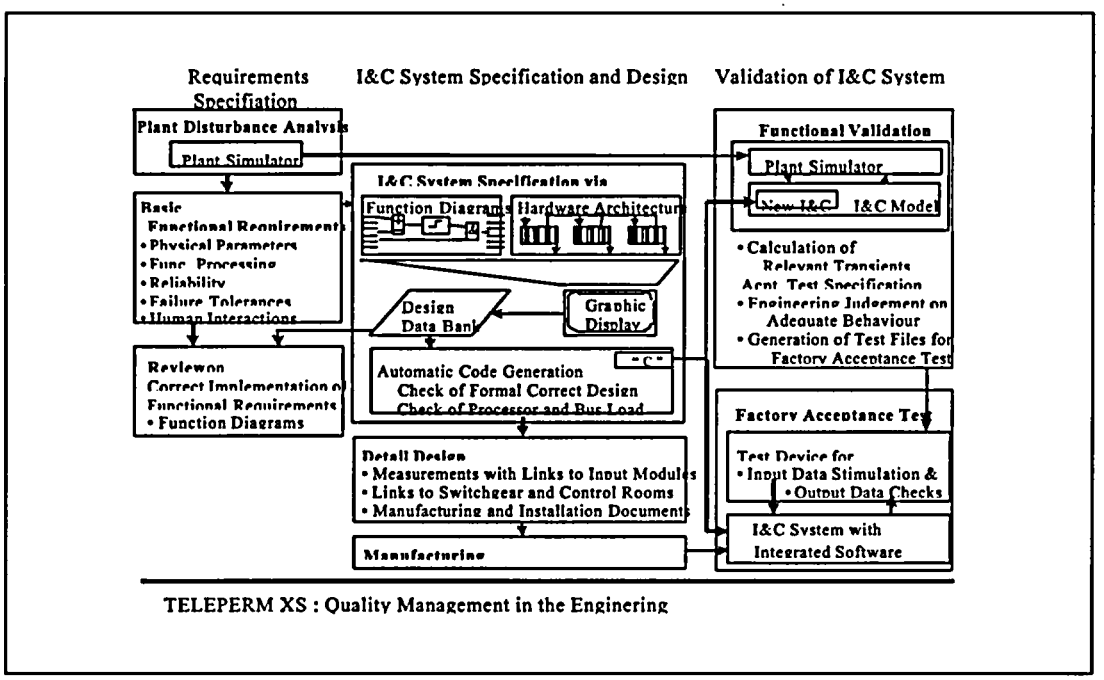


Figure 6-1: Quality of the TXS Engineering Process

SPACE's most effective technique for eliminating design errors is the functional validation of the generated application software. For the functional validation, the generated application software (not only the code for the designed functionality but the complete code for the redundant system, including communication between redundant processors) is linked into a simulation environment (e.g., on a powerful workstation) and then checked by computing the relevant design transients. The functional validation process can also be used to generate the input/output data test files for the factory acceptance tests.

6.2.2 Formalized Engineering Process

The configuration of plant-specific application software is generally considered the most error-prone activity during the implementation of safety related I&C systems. For this reason, the production of application software is strongly formalized with the TXS system (see Figure 6-2). In this way, problems related to individual working methods of the I&C staff members can effectively be avoided. Not only the production but also the verification process can be automated to a remarkably high degree. In addition to the function described, the tools required for verification and validation have also been integrated into SPACE, so that its function scope is far greater than that of any previously known engineering aid.

With SPACE, the following process model is used to develop plant-specific application software: the task specifications are mainly defined by mechanical engineers, process engineers, and physicists in prose, diagrams, equations, and tables and are passed on to the I&C specialists in this form. These problem definitions are read and further dealt with by I&C specialists - i.e., control engineers, communications engineers, physicists, computer engineers, and mathematicians. Queries for better understanding develop into system discussions. The I&C specialists then prepare all the data and information in a predefined way before using the editor of the SPACE engineering system to specify the I&C functions in the form of function diagrams. These function diagrams with well-defined presentation conventions can be read and understood by the parties that originated the task specifications for verification purpose and also serve as documentation for the customers.

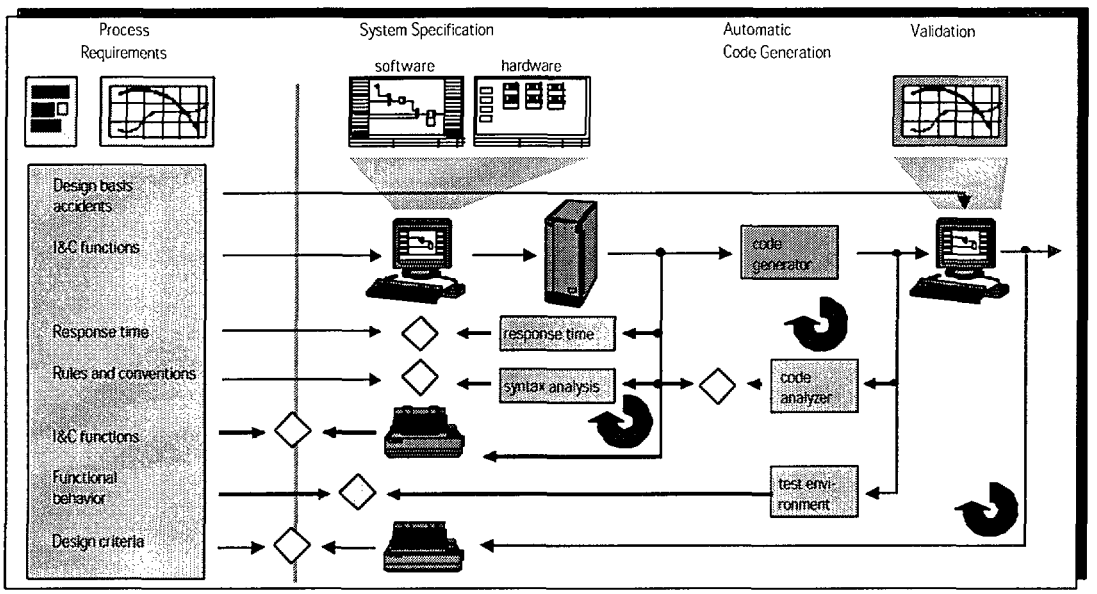


Figure 6-2: Formalized Engineering Process

Once the specification is complete, it can be checked automatically according to various criteria using analysis tools. This analysis includes such important characteristics as completeness and the absence of ambiguity. This has been made possible by the use of rigorously formal methods. The formally correct specification is then passed on for verification to the originators of the requirement specification who are also responsible for its release. For the quality of the application software, it is of decisive significance that the application software is automatically derived from the formal specification by qualified generators. Since an automatic tool generated the software, it is possible to verify the consistency of the generated code with the formal specification using a second automatic tool. One consequence of this method is that quality verification of the code generator can be kept economically viable.

After this verification step, the automatically generated code can be tested with the Simulation Based Validation Tool (SIVAT). This tool uses the exact same generated application code as generated for the target system. It creates a test environment on the engineering workstation computer, which facilitates a comprehensive functional testing of the generated application code. The behavior of the application functions to freely configurable input signal transients can be tested and I&C faults, such as communication or equipment failures, can be simulated. The validation tests are supported by a graphical user interface that also provides means for documentation of the validation tests, such as plots and listing. In order to find errors in the application functions, SIVAT also provides the capability to open dynamic SPACE function diagrams with live data for the simulation. A real process simulation model can be added to SIVAT, in order to provide more realistic process feedback to the simulation.

6.3 SYSTEM SOFTWARE DESIGN PRINCIPLES

In the software, a failure dependent on the loading profile cannot be ruled out because the effect of any fault in the application software depends on the loading profile. This applies to errors in the fluid system requirements, as well as to specification or implementation errors in the software. To avoid such errors, the following measures are taken:

- The application software is developed in documented phases and is automatically created by qualified generators.
- The automatically generated code has a very simple structure that always remains the same.
- The source code executed in the target system is also used for simulation of the I&C functions on the Engineering Workstation. One compiler for the Engineering Workstation is used to develop the executable programs for the simulation environment and another compiler for the target system is used to develop the executable programs on the target system. In the course of the functional tests and the system tests, it is verified that the programs produce the same result both on the target system and in the simulation environment.
- Compiler, linker and locater are always used in the same way with call parameters always remaining the same.
- Functions block modules are used. These modules operate with a defined data exchange. All data operations are subjected to validity checks.
- The reproducibility of this automated procedure has decisive advantages over all other methods in which programming is carried out directly by the engineer and supplemented with quality assurance:
- The scope of the basic software, i.e., the function block modules and their connection rules, remains small and manageable.
- The re-use of function blocks means that the basic software can be used for a large number of applications.
- The generated code can be used directly to perform closed-loop simulation in conjunction with suitable partial simulators (if available).

The system design is based both on principles of fault exclusion and restricting the consequences of failures to the safety system.

Even here, two diverse measures are taken to ensure that the consequences of a fault are restricted. First, the system design ensures that different loading profiles affect only the associated application function and not the system functions. This is achieved by the following design features:

- The entire application software functions cyclically.
- Process-dependent interrupts are excluded both in the user software and in the operating software to ensure cyclic processing of the user software in a deterministic way.
- The program control in the system services is completely independent of the loading. This means that there is neither a direct dependency, for example, in the form of process data dependent function calls, or an indirect dependency via the use of resources (e.g., CPU load).
- The operations on process signals are performed only in function block modules whose quality has been verified.
- The definition ranges of input signals for function blocks have been selected such that input data combinations that are possible from the A/D converter cannot cause values to fall outside the defined range.
- The function block modules automatically check the values of the input data prior to critical operations.

The design is subjected to a rigorous Independent Verification and Validation (IV&V) Process during all phases of the design to assure the following:

- Earliest possible detection and correction of design errors
- Enhancement of the quality and reliability of the I&C system
- Quick evaluation of the consequences of planned modifications

A requirements traceability matrix is used to ensure software requirements are faithfully translated to design documents and that all software requirements are tested.

The second measure is to confirm the effectiveness of the design features described above by verifying freedom from interference during the plant-independent system test. The effectiveness of the fault-confinement measures has been verified in a plant-independent system test with the participation of German Reactor Safety Association (GRS-ISTec) and the German Technical Inspection Agency (TÜV-Nord). The fundamental feature on which verification was based is that the various fluid-system-independent application functions and the associated system services are executed cyclically and invariably in time, irrespective of load. To observe normal operation of the TXS system, one of the independent user functions is fed with meaningful fluid system input data to allow the expected output signals to be checked, while the remaining functions are supplied with random input data that have no logical connection with the fluid system process to be controlled. Stochastic input data are used for this test. The

aim of the tests is not to determine "correct" results from deliberately meaningless and inconsistent input data but to verify that correct processing of the user function is not impaired by random and abnormal loading profiles. These tests demonstrate that the software generated with SPACE for the TXS system has no interference on the system behavior and in particular does not cause exceptions, irrespective of the trajectories of the input data. At the same time, freedom from interference between independent application functions is also verified in the above tests. Independent application functions are therefore only coupled via their common processor system.

In this way, a degree of independence is verified which is comparable, for example, to that existing between "independent" protection functions in the proven hardwired technology, where the functions are installed with the same modules in the same cabinet and fused via a single cabinet fuse, but are independent in I&C terms. This is an inherent characteristic of hardwired protection systems but it must be designed into digital I&C systems. In addition, all important system features of TXS are proven in the plant-independent system test. These important design features which are validated are as follows:

- Effectiveness of component failure detection.
- Effectiveness of independent tripping channels to ensure defined failure behavior.
- Correctness of response time behavior.
- Correct behavior during test and diagnosis and consequently the system repairability.
- Effectiveness of the barriers at preventing an inadmissible change of the operating mode.

6.4 CONFIGURATION MANAGEMENT

Requirements and procedures necessary for the configuration management activities for the system development are controlled by engineering procedure. It identifies the software configuration management requirements and establishes the methodology for generating configuration identifiers, controlling engineering changes and maintaining status accounting during the design and development of software configuration items. It is applied to all software and associated documentation of the TXS system. The content of the engineering procedure is summarized below:

6.4.1 Management of Configuration Items

Configuration identification is applied to all software code and associated documentation. A software configuration is made up of software elements and the associated documentation. A configuration item is an identifiable element of a software configuration, which may be an individual document, or a whole software configuration.

The label of each configuration item is unique. A version number is assigned to each configuration item. Baselines are established for the control of design, product and engineering changes. The product authority defines baselines. Throughout the development life cycle, at the discretion of the configuration control board, releases are performed. Releases of a software configuration are defined by a list that identifies all items of the configuration. The procedure to change configuration items consists of the following steps:

1. Change Request
2. Evaluation of the request by the development group
3. Proposal how to perform a change
4. Decision about the change
5. Performing the changes (including test and update of the documentation)

6.4.2 Configuration Control

Software configuration management and change control is applied to all documents and code. Control is affected through the implementation of the configuration identification, the change control, and status accounting functions. Changes are initiated by a formal change request. A change request includes the following information:

1. Identification of the request, product, date, and author
2. Specification of the request including the reason
3. Identification of the configuration item
4. Category of the request
5. Behavior of the product as it is
6. Requested behavior of the product

Change requests are analyzed and evaluated. As a result, a formal change proposal is generated. This proposal provides methodologies of how to perform the changes and the associated consequences. The change request forms the basis for the decisions taken by the project management. The decision is documented by a development order. After development, test, and updating of the product related documents, the change process is finished by a formal document, which contains a short report about the changed configuration item.

The measures described apply to the hardware and software elements of the TXS system and assure that each TXS application project is based on a qualified and well-configured set of building blocks of the system.

The project specific configuration management activities are supported by the SPACE engineering tool set. These activities can be divided into two basic tasks:

- Assure that only qualified hardware and software components of the system are used (versions, releases).
- Assure that the application software is consistent with the application specific requirements.

6.4.2.1 Management of the System Software Configuration

The configuration of the system software components installed on the SPACE Engineering Workstation has to be checked prior to each code generation process, in order to make sure that the correct tools are used for code generation and the correct system software components are linked to application software. The software version of each system software component running on a TXS function computer can be read back by the Service Unit at any time. The SPACE engineering tools support both functions and the methods are described in engineering procedures.

6.4.2.2 Management of the Application Software Configuration

The application software configuration is controlled on five different levels (Figure 6-3):

1. I&C requirements specification
2. Functional specification in the SPACE database
3. Source code of the application software generated by the SPACE code generators
4. Executable code containing system and application software
5. Software stored on the TXS CPU's FEPROM

The application software modification process from application software configuration version J to J+1 is shown on Figure 6-3.

- Starting point of any software modification is a modification of the I&C requirements specification (i.e., design change package).
- SPACE database version J presents the currently implemented status of the I&C system specification. A copy of this database is made identifying the configuration (CRC check sums).
- The design modifications are implemented in the SPACE database using the function diagram editor and creating database version J+1.
- All modifications made are logged in the database. Thus, printouts can be made of the modified diagrams and modification listings can be created. This allows verifying the changes made in the database.
- The application program source code version J was generated during the last code generation process. Its configuration is identified (CRC check sums).
- Using the SPACE code generators (a) a complete new set of source code is generated or (b) new code is generated only for the modified parts of the

specification. In both cases code generation results in a new software version J+1. The new set of source code is identified using CRC check sum.

- SPACE tools allow the comparison of both sets of source code, in order to verify the modifications made.
- Using the SPACE compiler, linker and locator, the executable I&C code version J+1 is created consisting of the application code and the system software components. The new executable code is identified using CRC check sums.
- SPACE tools allow the analysis of the configuration of the executable code reading the ID string information of the implemented software components. Thus, the modifications in the executable code can be compared with the intended I&C modifications.
- SPACE tools also predict the CRC check sums of the FEPROM segments on the CPU used by the generated code. The cyclic self-monitoring features monitor these check sums. Furthermore, the check sums can be recalculated and read back from the CPU at any time, in order to verify the identity of the implemented software.

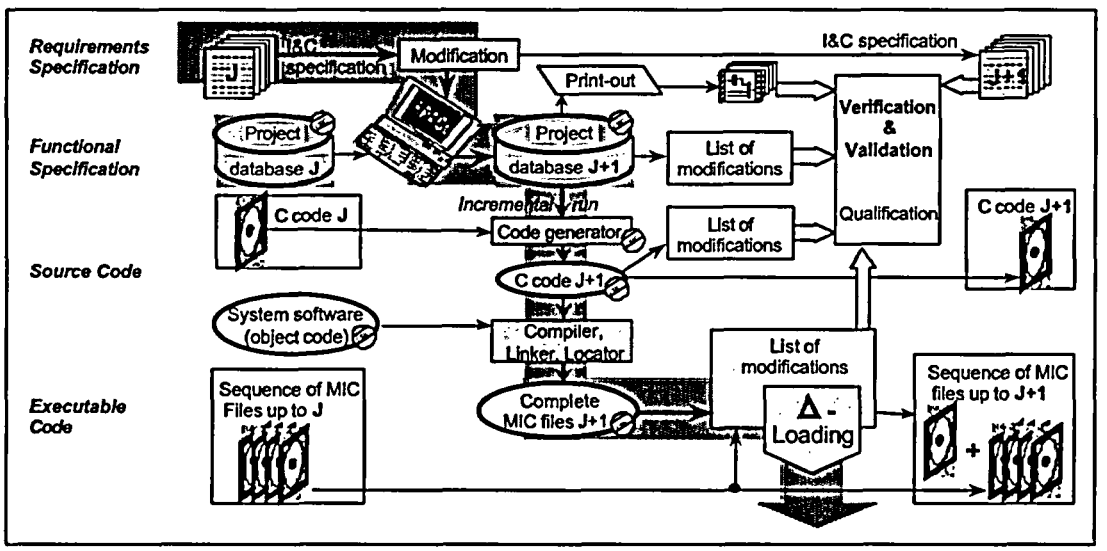


Figure 6-3: Configuration Management for Application Software Modifications

6.5 MONITORING AND TESTING

The self-monitoring features for TXS consist of the self-test, which is a start-up self-test, which confirms operation upon system initialization, and a cyclic self-test. There is also an exception handler, error detection by the runtime environment (RTE), cabinet monitoring devices, and engineered monitoring features. The self-monitoring features cover several important runtime environment aspects. Other features consist of CRC sum, message age monitoring, message header check, plug-in monitoring, computing time monitoring, cyclic self-test monitoring, and master/checker result monitoring on the

TXS voters. The RTE also increments the cycle counter. The cycle count at the time of transmission is appended to every message. This information is used by the receiver to monitor the validity of the message and the correct function of the transmitter.

The self-monitoring software performs a sequence of checks on the various hardware components of the processing module. These checks include a RAM test, an EEPROM test, and a watchdog timer test. This activity is performed during time intervals when the cyclic processing of the functional diagram modules is inactive. This is a continuous check and is monitored by the RTE. The exception handler receives the errors, stores them, and responds properly. The watchdog timer is reset every cycle to a certain value that is greater than the activation cycle for the RTE cycle time. If the RTE does not terminate correctly because of a fault, the watchdog timer times out and generates a hardware interrupt request. This request activates the interrupt service in the exception handler, saves the current state of the processor for subsequent analysis, and places the processor in a defined fault state. The first watchdog timer fault is considered a transient, and the CPU is automatically rebooted which causes a complete start-up self-test to be executed. This provides for an in-depth check of the CPU hardware. If the watchdog timer times out again, then the complete I&C sub rack has to be reset via manual means. A complete check of the failure information is performed before the reset.

Another software common-mode failure prevention measure is the testing required by Surveillance Requirements in the Technical Specifications. Surveillance requirements are requirements related to test, calibration, or inspection to assure that the necessary quality of systems and components is maintained, that facility operation will be within safety limits, and that the limiting conditions for operation will be met. Technical Specification 3.3.1, "Reactor Trip System (RTS) Instrumentation", and 3.3.2, "Engineered Safety Features Actuation System (ESFAS) Instrumentation", identifies the specific testing and frequencies associated with the RTS and ESFAS. Changes to these Technical Specifications as well as other instrumentation Technical Specifications will be requested, as appropriate, to define the testing requirements for the TXS system.

6.6 OPERATING HISTORY

A mature operating history for the TXS system, which is on the order of more than 15 million accumulated hours for the processing and communication modules has resulted in no failures that have degraded plant operation. To date, all of the reported failures have been hardware related with no reported software failures occurring during plant operation.

6.6.1 Reliability Analysis

For each of the hardware components, a comprehensive reliability analysis has been performed (Reference /30/), determining the overall failure rates of modules and sub-modules based upon the Siemens standard SN29500 utilizing Arhenius calculations. For some of the components, actual rather than analytical reliability data is shown in

Table 6-1. I&C applications are designed in a way, that they meet the reliability requirements based on the theoretical reliability data. Operating experience, however, has shown that these figures are overly conservative. Based on its comprehensive failure reporting system, FANP plans to use operating experience data in order to adjust module failure rate data.

Table 6-1: TXS Module Reliability/Availability Data at 83°F

Components	Failure Rate [1/h]	MTBF [years]	MTTR [h]	Availability [%]
Processing Module / CPU Including Communications	1.4×10^{-6}	82	24[1]	99.99
I/O Modules	6.2×10^{-7} – 2.1×10^{-6}	54 – 182	24[1]	99.99

[1] Values used for safety analysis (worst case assumes no qualified personnel on site)

6.6.2 Failure Modes and Effects Analysis

During the baseline qualification of TXS performed in Germany, detailed Failure Modes and Effects Analysis for each TXS module were performed. During each application project, FANP provides additional documentation on the effects of each defined module-based failure mode (e.g., output signal fail-high, fail-low, fail-as-is) on the application function.

6.6.3 Mean Time Between Failure

The Mean Time Between Failures (MTBF) for the CPU processing module is estimated to be 259 years based on actual field data with a Mean Time to Repair (MTTR) of 24 hours, which is significantly greater than the analytical values in Table 6-1 above. The availability is greater than 99.99% (Reference 30). New processing and communication modules, SVE2 and SCP2, which will be installed, are generally based on the same hardware components but a new processor. The components have been selected to achieve the same or better reliability than the original SVE1 and SCP1 processors. The occurrence of no problems identified to date for the first applications of these new modules in other projects supports this assertion. Any residual uncertainty when evaluating the potential for software common-mode failures has been eliminated by the above process.

6.7 System Aging Considerations

For system failures due to aging, design errors or manufacturing defects can cause common-mode failure after a certain time but independently of the input profiles. Failure of the hardware can result from dependent failures due to aging caused by manufacturing defects. Because safety I&C systems are designed as responsive systems, actions are derived only from process signal inputs and from operator requests. Therefore no equipment for time (e.g., time switches) processing is used.

Design errors only have an effect with respect to the mechanisms considered here in that they can cause more frequent failures due to aging and therefore result in aging-induced system failure over a long time. A failure due to aging is always caused by a time-dependent physical chemical process that changes the characteristics of the components. The times at which failures occur are not correlated in time because the physical and chemical processes always progress differently as a result of individual manufacturing tolerances and differing ambient conditions. This means that an almost simultaneous failure of several components as a result of this mechanism can be ruled out.

Aging-induced software failure is only possible if there are time dependencies in the software in the form of some type of long-term integrator that maps itself into the variable data in some way. Two diverse mode measures are implemented within TXS to prevent time-dependent failures. The first prevention measure is that all types of long-term integrators have been explicitly avoided during software development. There is no real-time clock but only short-time counters with a counting cycle of approximately one hour for checking the sequence of messages. These short-time counters are not correlated between redundant items of equipment. The second is that the operating system is static so that slow, time-dependent consumption of resources can be ruled out. Communication also functions without dynamic buffers. This means that time-dependent failures that only manifest themselves after hundreds of thousands of operations are ruled out by the design.

6.8 QUALITY AND STANDARDS APPLIED TO TXP SYSTEMS

The following provides a break down of the applicable standards applied for non-safety systems, in a listed form (see Figure 6-4). It outlines the standards which are taken into account for the development of TXP. The list summarizes the considered standards for each component of TXP. For the components only the relevant standards of the list apply.

System concept	System reliability	System test	System quality assurance	System documentation
VDI / VDE 2880 VDI / VDE 3649 IEC 987 IEC 1131-1 IEC 1131-2 DIN / VDE 0801 IAEA-50-SG-D8	VDI / VDE 2180/2 VDI / VDE 3691 DIN / IEC 300 DIN 31000	VDI / VDE 2180/4	VDI / VDE 3691 ISO 9000-3 ISO 9001 ISO 9004	VDI / VDE 3559 DIN 66230 DIN 19239

Hardware requirements	Hardware quality procedures	Hardware documentation	Hardware qualification	Hardware reliability
IEC 38 IEC 381/1,2 IEC 721, IEC 664-1 IEC 664A, IEC 801/1-6 IEC 946 IEC 1131-1 DIN / IEC 654/1-3 DIN / VDE 0160	VDI / VDE 3540/1	VDI / VDE 3559	IEC 1131-2 IEC 68/2-01, 02, 03, 06, 14, 27, 30 IEC 801/2-6	SN 29500 DIN / IEC 409 DIN / IEC 605/1 DIN / IEC 605/3,2 DIN / IEC 706/1

Software requirements	Software quality procedures	Software documentation	Software qualification
VDI / VDE 2880/4 IEC 1131-3 DIN 19239 DIN / VDE 0116 DIN / VDE 0801 IEEE 830 IEEE 1016	IEEE 730 IEEE 828 ISO 9000-3	VDI / VDE 3559 DIN 66230 DIN 66231 DIN 66261 IEEE 829	IEEE 829 IEEE 1008 IEEE 1012 IEC 880

Figure 6-4: Applied Standards for TXP

Use of the above standards ensures the development process is managed and controlled to obtain quality and dependability similar to that in TXS systems.

7 DEFENSE-IN-DEPTH AND DIVERSITY

The TXS design is diverse and meets the acceptance criteria of BTP HICB-19. Section 5 provides a description of the TXS architecture and design features that prevent a software common-mode failure from disabling the successful operation of the RTS and ESFAS as well as other TXS-based systems shown on Figure 4-1, such as LSELS, MSFIS and EDG controls. Even without this TXS inherent design diversity, the design is such that there is adequate defense-in-depth to cope with a complete failure of the TXS based RTS and ESFAS for most events. A failure would need to entail two distinct or multiple software common-mode failures or an unknown common-mode failure other than software, to prevent RTS and ESFAS from functioning.

Certain systems comprising the four echelons of defense are diverse from the software for the TXS system. The I&C systems included in the four echelons of defense-in-depth consist of the control systems, the RTS, the ESFAS and the Monitoring and Indication System. In the defense-in-depth concept of the plant, the control systems, RTS, ESFAS, and Monitoring and Indication Systems represent the main line of defense. A second line of defense is provided by a combination of control systems, AMSAC, and manual controls. Although incredible, in the unlikely event the RTS and ESFAS were to become unavailable due to two different postulated software common-mode failures, the system architecture has been carefully designed to assure that the control systems, AMSAC and indications necessary for operator action remain available.

Acceptable defense-in-depth is provided through adequate independence and diversity between the RTS/ESFAS TXS systems and other I&C echelons of defense such as the control systems, certain plant safety systems, indications, alarms and read-outs, and manual actuation circuitry. In addition, the systems in place to meet the ATWS Rule (Reference /17/) continue to meet the diversity provisions of that Rule. Diverse equipment/systems are established that are not subject to the same common-mode failure and which, as a result, will provide a path for meeting the provisions of BTP HICB-19 as it relates to the FSAR/USAR Chapter 15 analyses. The discussion below highlights the systems that are considered to be diverse from the TXS RTS/ESFAS. Systems that are diverse for the TXS system and used in the Section 8 event assessment provide the defense-in-depth as discussed in the BTP HICB-19. Since numerous safety systems are to be TXS based, the defense-in-depth is provided by control system automatic actuations and/or safety system manual actuations with diverse indication, as well as from the inherent defense-in-depth built into each TXS system

7.1 DIVERSITY FEATURES BETWEEN TXS AND TXP SYSTEMS

The TXS system used in the safety systems and the TXP system used in non-safety systems have been evaluated for diversity in the categories of design diversity, human diversity, equipment diversity, software diversity, functional diversity, and signal diversity.

The purpose of providing this evaluation is to highlight the diversity features between these two systems and to take credit for the successful operation of TXP based systems provided in the first echelon, control systems.

Table 7.1 below summarizes the diversity features between the TXS and TXP systems (Reference *[7]*).

CATEGORY	***ATTRIBUTE***	***TXS***	***TXP***
Design Diversity	Architecture	Totally different structure, arrangement and communication of components from that used for TXP	Totally different structure, arrangement and communication of components from that used for TXS
Human Diversity	Design organization	Framatome ANP GmbH, Inc.	Siemens PG L, SWPC
Human Diversity	Engineering management	Framatome ANP GmbH, Inc.	Siemens PG L, SWPC
Human Diversity	Designers and programmers	Framatome ANP Inc.	Siemens PG L, SWPC
Human Diversity	Testers and installers	Framatome ANP Inc.	Siemens PG L, SWPC
Equipment Diversity	Input/Output boards	Derived from Simatic S5	Proprietary FUM, SIM modules
Equipment Diversity	Microprocessor CPU	[ ]	Simatic S5 CPU 948R
Equipment Diversity	Bus structure	K32 Bus	Redundant cabinet internal bus for FUM modules, Profibus for SIM/ET200 connection
Software Diversity	Computer language	[ ]	Step 5; MC5 Code generator and Assembler/Linker on ES 680
Software Diversity	Operating system	MICROS – Siemens Design	BESY
Software Diversity	Software development tools	SPACE on LINUX	ES 680, ES685 on HP-UX, SCO-UNIX
Software Diversity	Software database	ORACLE	INGRES
Software Diversity	Software Validation tools	SIVAT Simulation and Validation Tool, RETRANS – Siemens Design	SIMIT Simulator
Software	Algorithms, logic,	Algorithms, logic, and	Algorithms, logic, and

CATEGORY	ATTRIBUTE	TXS	TXP
Diversity	and program architecture	program architecture are different, different function block implementation, different database structure than the one implemented for TXP.	program architecture are different, different function block implementation, different database structure than the one implemented for TXS.
Software Diversity	Timing and order of execution	Deterministic behavior (no process interrupts), Unsynchronized CPU timing, Real Mode, Static Memory Allocation	Non-deterministic behavior (process interrupts are used), Synchronized CPU timing, Dynamic Memory Allocation
Functional Diversity	Response Time Scale	40-50 ms cycle time	100-200 ms cycle time (in general)
Functional Diversity	Functional Purpose	Reactor Trip and ESF Actuations, Safety Control functions	Plant Control and Information Systems
Signal Diversity	Reactor or Process Parameters	Reactor parameters of temperature, pressure, flow, and level are sensed by Protection Sets analog electronic modules and provided via isolated outputs to TXP.	Parameters are received from the Protection Sets isolated outputs into TXP A/D modules or sensed by TXP transmitter modules.

Table 7.1 Diversity Features Between the TXS and TXP System

A review of this effort yields the following major diversity features between the two systems:

- The design architectures are completely different.
- The design organization, management, designers, programmers, and testing engineers are different.
- The microprocessor CPUs, input/output circuit boards and bus structure are from different manufacturers.
- The software languages are different.
- The software operating systems are different.
- The software development tools are different.
- The software validation tools are different.

- The software algorithms, logic, program architecture, timing, and order of execution are different.
- The application programs are functionally diverse.

The design architecture diversity attribute is a powerful type of diversity because it requires the use of different configurations and functionality with different approaches and arrangements. The equipment diversity attribute of different microprocessor CPU architecture is also a powerful type of diversity because it requires the use of different printed circuit board designs, bus structures, CPU architectures, compilers, linkers, and other auxiliary programs. Management diversity also has a significant effect on diversity because management controls the resources applied and the corporate culture under which designers and programmers work. Lastly, software diversity as shown above, leads to different algorithms, logic, program architecture, timing, order of execution, operating systems, and languages. Individually, these are all strong arguments for proving diversity. When taken together, they clearly show that the TXS and TXP systems are truly diverse.

The designed control systems, which consist of non-safety related digital equipment, are clearly diverse and independent from the TXS system. The remaining analog-based control systems are also diverse from RTS and ESFAS and not subject to any type of software failure. However, certain inputs to these controls systems are provided by the TXS system. This is depicted in Figure 4-1, which clearly shows that a TXS software common-mode failure will not affect these inputs to the control systems. As such, actions to mitigate any event using systems that are not reliant on TXS meets the diversity guidance within BTP HICB-19 and NUREG/CR-6303.

If any control systems are modified in the future along the lines of a digital design, then the diversity arguments presented in this report will be applied, and the control blocks will have to be reevaluated.

7.2 CONTROL SYSTEMS DIVERSITY

The following is a listing of control systems within the plant design that are diverse from the RTS/ESFAS TXS system and are not subject to the same common-mode failure. A description of these control systems can be found in the FSAR/USAR Section 7.7. The following systems are not TXS-based and would not be subject to the same software common-mode failure. Where the existing plant functional design requires the sharing of a signal source between the RPS and the control systems, the TXS architecture provides for an isolated analog output signal from the RPS to the control system. With this strategy, a postulated software common-mode failure in the TXS RPS cannot cause a control system response that would require a reactor trip or engineered safety feature actuation.

7.2.1 Reactor Control System

Callaway Plant

This system enables the nuclear plant to accept a step load decrease of 10 percent and a ramp decrease of 5 percent per minute over the entire power range without reactor trip, steam dump, or pressurizer relief actuation. It also maintains T_{avg} within prescribed limits by creating bank demand signals.

WCGS

This system enables the nuclear plant to accept a step load increase or decrease of 10 percent and a ramp increase or decrease of 5 percent per minute within the load range of 15 percent to 100 percent without reactor trip, steam dump, or pressurizer relief actuation. It also maintains T_{avg} within prescribed limits by creating bank demand signals.

7.2.2 Rod Control System

The Rod Control System that provides for reactor power modulation by manual or automatic control (insertion only for the Callaway Plant) of control rod banks in a pre-selected sequence and for manual operation of individual banks consists of two parts.

- The first part, automatic rod control is controlled by TXS. The initiation part is included in the NSSS-control system and is not TXS based.
- The second part performs the computation of the signals and distribution with the correct timing to the power cabinets, using the TXS voter system. This part has a simple functionality as described in Section 7.1 and is totally independent and separate from any other TXS system.

7.2.3 Pressurizer Pressure Control System

This system maintains or restores the pressurizer pressure to the design pressure following normal operational transients that induce pressure changes by control of heaters and spray in the pressurizer. It provides steam relief by controlling the power relief valves. In addition, there are pressurizer safety valves that automatically provide pressure relief upon reaching its relief setpoints.

7.2.4 Pressurizer Water Level Control System

This system establishes and maintains the pressurizer water level within specified limits as a function of the average coolant temperature. Level changes are produced by means of charging flow control (manual or automatic) as well as by manual selection of letdown orifices.

7.2.5 Steam Generator Water Level Control System

This system establishes and maintains the SG water level within predetermined limits during normal operating transients. It regulates the feedwater flow rate so that under operational transients the water level for the SG does not decrease below a minimum value. This control can be manual or automatic through the use of feedwater control valves.

7.2.6 Steam Dump Control System

This system permits the plant to accept a sudden loss of load without incurring a reactor trip. Steam is dumped to the condenser or into the atmosphere. The system also ensures that stored energy and residual heat are removed following a reactor trip and maintains the plant at no-load conditions, permitting a manually controlled cooldown of the plant.

7.2.7 Incore Instrumentation

The incore instruments provide information on the neutron flux distribution using a discontinuous working Flux Mapping System.

7.3 ATWS Mitigation System Actuation Circuitry

AMSAC was installed in compliance with 10 CFR 50.62, "Requirements for Reduction of Risks from ATWS Events for Light Water Cooled Nuclear Power Plants," (Reference /15/) to improve the capability to mitigate an anticipated transient without scram (ATWS) event. The AMSAC is part of another independent and diverse block, implemented with equipment diverse from TXS, and will continue to meet the ATWS Rule. The AMSAC equipment becomes very important when used to provide an independent and diverse protective action as a backup to the TXS RTS protective features.

AMSAC functions to automatically initiate an AFW actuation signal (motor-driven and turbine-driven) and turbine trip under ATWS conditions. An ATWS is indicative of the RTS failure to take actions when required (e.g., reactor trip, turbine trip).

In the most severe ATWS scenarios, the most limiting condition was found to be RCS pressures approaching the 3200 psig limit corresponding to the ASME Boiler and Pressure Vessel Code. This condition occurred in the Complete Loss of Normal Feedwater ATWS, and the Loss of Load ATWS. Generic studies showed acceptable consequences would result if nominal conditions (as allowed by the NRC) were assumed, provided that the turbine trips and AFW is initiated in a timely manner.

Normally the turbine trip and AFW signals would be initiated by the RPS. If however, the common-mode failure that prohibited the reactor trip were in the RTS, it would also prohibit the turbine trip and AFW signals. AMSAC was thus devised to initiate the

turbine trip and AFW signals on an ATWS. Where the existing plant functional design requires the sharing of a signal source between the RPS and the AMSAC, the TXS architecture provides for an isolated analog output signal from the RPS to the control systems. With this strategy, a postulated software common-mode failure in the TXS RPS cannot cause a control system response that would require a reactor trip for any ATWS event.

7.4 SYSTEM MANUAL ACTUATION/MONITORING DIVERSITY

In the current and upgraded I&C concept, the manual initiation of the reactor trip is performed by hard-wired hand switches on the MCB, bypassing the TXS trip logic, and directly connecting to the control circuits of the trip breakers. Also, in the current I&C architecture, most NSSS ESF manual actuations come directly to SSPS Master Relays independent of the SSPS logic. Some manual actuations, such as SI, come directly to the Master, but use Slave Relays to multiply the SI signal to MSFIS, BOP ESFAS, LSELS, and so on. For reasons of diversity and independence, any manual actuation path that uses the TXS CPUs cannot be credited as a diverse path for manual initiations that are required as a result of the D-in-D&D assessment, as these actuation paths would pass through the programmable portion of the TXS. Therefore, an independent, diverse manual initiation path is implemented in conjunction with the TXS system.

[

]
A part of the information from the safety systems to the control systems is acquired by the TXS system (i.e., Category 1 and some Category 2 safety related PAMS parameters) and transferred using isolation devices directly hardwired to the control system (Section 5.9), bypassing the TXS software (Figure 5-1). Some Category 2 and all Category 3 PAMS parameters are available directly through the control systems that are diverse and independent from TXS. FANP assures that all monitoring/indication that is necessary as a result of the D-in-D&D assessment is provided in an acceptable diverse and independent manner (as discussed above). The TXS system design provides the outputting of the necessary monitoring information after signal conditioning but prior to the TXS system input modules through qualified isolation devices where necessary (Figure 4.2). The indications are addressed in Sections 4 and 5, and are diverse and independent from the RTS/ESFAS TXS software.

In conclusion, the required monitoring and indication information is not subject to a TXS related software common-mode failure since this information is obtained prior to TXS processing, and therefore, it is independent and diverse from the TXS software.

8 SPECTRUM OF TRANSIENTS AND ACCIDENTS

This section evaluates the impact on the FSAR/USAR accidents and transients of replacing the analog RTS and the ESFAS with a digital computer-based system, TXS.

All the events described in FSAR/USAR Chapter 15 were selected for qualitative re-evaluation. Other accidents were also considered relevant for this evaluation: the containment functional design described in FSAR/USAR Chapter 6.2.1 and the equipment environmental qualification issues described in FSAR/USAR Chapter 3.0 were considered. Together, these events are considered to be the full set of events that needed to be considered in assessing the impact of the TXS. The FSAR/USAR events that were re-evaluated are listed below:

- (FSAR/USAR 15.1.1) Feedwater System Malfunctions that Result in a Decrease in Feedwater Temperature
- (FSAR/USAR 15.1.2) Feedwater System Malfunctions that Result in an Increase in Feedwater Flow
- (FSAR/USAR 15.1.3) Excessive Increase in Secondary Steam Flow
- (FSAR 15.1.4) Inadvertent Opening of a Steam Generator Relief or Safety Valve
- (USAR 15.1.4) Inadvertent Opening of a Steam Generator Atmospheric Relief or Safety Valve
- (FSAR/USAR 5.1.5) Steam System Piping Failure
- (FSAR/USAR 15.2.1) Steam Pressure Regulator Malfunction or Failure that Results in Decreasing Steam Flow
- (FSAR/USAR 15.2.2) Loss of External Electrical Load
- (FSAR/USAR 15.2.3) Turbine Trip
- (FSAR/USAR 15.2.4) Inadvertent Closure of Main Steam Isolation Valves
- (FSAR/USAR 15.2.5) Loss of Condenser Vacuum and Other Events Resulting in Turbine Trip
- (FSAR 15.2.6) Loss of Nonemergency AC Power to the Station Auxiliaries
- (USAR 15.2.6) Loss of Nonemergency AC Power to the Station Auxiliaries (Blackout)
- (FSAR/USAR 15.2.7) Loss of Normal Feedwater Flow
- (FSAR/USAR 15.2.8) Feedwater System Pipe Break
- (FSAR/USAR 15.3.1) Partial Loss of Forced Reactor Coolant Flow
- (FSAR/USAR 15.3.2) Complete Loss of Forced Reactor Coolant Flow
- (FSAR/USAR 15.3.3) Reactor Coolant Pump Shaft Seizure (Locked Rotor)
- (FSAR/USAR 15.3.4) Reactor Coolant Pump Shaft Break
- (FSAR/USAR 15.4.1) Uncontrolled Rod Cluster Control Assembly Bank Withdrawal from a Sub critical or Low Power Startup Condition

- (FSAR/USAR 15.4.2) Uncontrolled Rod Cluster Control Assembly Bank Withdrawal at Power
- (FSAR/USAR 15.4.3) Rod Cluster Control Assembly Misalignment (System Malfunction or Operator Error)
- (FSAR/USAR 15.4.4) Startup of an Inactive Reactor Coolant Loop at an Incorrect Temperature
- (FSAR/USAR 15.4.5) Malfunction or Failure of the Flow Controller in a BWR Loop that Results in an Increased Reactor Coolant Flow Rate *(The Callaway Plant and WCGS are Pressurized Water Reactors (PWRs). This BWR malfunction or failure is not applicable. No evaluation is performed.)*
- (FSAR/USAR 15.4.6) Chemical and Volume Control System Malfunction that Results in a Decrease in the Boron Concentration in the Reactor Coolant
- (FSAR/USAR 15.4.7) Inadvertent Loading and Operation of a Fuel Assembly in Improper Position
- (FSAR/USAR 15.4.8) Spectrum of Rod Cluster Control Assembly (RCCA) Ejection Accidents
- (FSAR/USAR 15.5.1) Inadvertent Operation of ECCS during Power Operation
- (FSAR/USAR 15.5.2) CVCS Malfunction that Increases Reactor Coolant Inventory
- (FSAR/USAR 15.6.1) Inadvertent Opening of a Pressurizer Safety or Relief Valve
- (FSAR/USAR 15.6.2) Break in Instrument Line or Other Lines from Reactor Coolant Pressure Boundary that Penetrate Containment
- (FSAR 15.6.3) Steam Generator Tube Failure
- (USAR 15.6.3) Steam Generator Tube Failure (SGTR)
- (FSAR/USAR 15.6.4) Spectrum of BWR Steam System Piping Failures Outside of Containment *(The Callaway Plant and WCGS are Pressurized Water Reactors (PWRs). This BWR malfunction or failure is not applicable. No evaluation is performed.)*
- (FSAR/USAR 15.6.5) Loss of Coolant Accidents Resulting from a Spectrum of Postulated Piping Breaks Within the Reactor Coolant Pressure Boundary
- (FSAR/USAR 15.7.1) Radioactive Waste Gas Decay Tank Failure
- (FSAR/USAR 15.7.2) Radioactive Liquid Waste System Leak or Failure
- (FSAR/USAR 15.7.3) Postulated Radioactive Releases Due to Liquid Tank Failures
- (FSAR/USAR 15.7.4) Design Basis Fuel Handling Accidents
- (FSAR/USAR 15.7.5) Spent Fuel Cask Drop Accidents
- (FSAR/USAR 15.8) Anticipated Transients Without Scram
- (FSAR/USAR 6.2.1) Containment Functional Design
- (FSAR/USAR 3.0) Design of Structures, Components, Equipment, and Systems

The evaluation methodology allowed the responses to FSAR/USAR transients and accidents to be classified into four categories:

Category 1 – The RTS and ESFAS are not actuated in the FSAR/USAR event, resulting in no impact.

Category 2 – The event is terminated successfully by the unaffected RTS and ESFAS functions (half channel capacity) through either automatic or manual actions.

Category 3 – The event is bounded by another event.

Category 4 – Further work is required to demonstrate successful event mitigation, such as quantitative analysis, event simulations, additional justifications, or plant modifications.

The listed FSAR/USAR events were qualitatively evaluated, and the conclusion was reached that since the RTS and ESFAS remain available concurrent with a worst-case common-mode failure, albeit at half-capacity, the results of the current licensing-basis FSAR/USAR Safety Analyses continue to be met. The capability to achieve acceptable hot shutdown and cold shutdown conditions continues to be met for all safety requirements given any of the postulated initiating events concurrent with a software common-mode failure to the TXS system. Therefore, all events were classified in the first three categories such that no additional actions per Category 4 were determined necessary.

The TXS system design provides for inherent system diversity by using certain architectural and design features. The architectural design and features eliminate the potential for a software common-mode failure within all channels of the TXS system. The architecture and design features are discussed in more detail in Section 5 of this report.

As is described in previous sections of the report, the TXS is designed to provide each function provided by the original RTS and ESFAS. TXS also is designed with sufficient diversity and redundancy so that the reliability of each function of the analog RTS and ESFAS is maintained. The D-in-D&D assessment demonstrates that the proposed digital I&C upgrade is fault tolerant and extremely resistant to software common-mode failures.

Even though software common-mode failure may be possible within identical software blocks, it is not possible for such a failure to occur at a system-wide level within the entire TXS system design. [

]

When considering best-estimate realistic assumptions (refer to Section 3) and the design of the digital computer-based TXS system, it was determined that the I&C Digital Upgrade meets the following BTP HICB-19 (Reference /1/) acceptance criteria:

1. For each anticipated operational occurrence in the design basis occurring in conjunction with each single postulated common-mode failure, the plant response calculated using best-estimate (realistic assumptions) analyses should not result in radiation release exceeding 10% of the 10 CFR 100 guideline value, or violation of the integrity of the primary coolant pressure boundary. The applicant/licensee should either (1) demonstrate that sufficient diversity exists to achieve these goals, or (2) identify the vulnerabilities discovered and the corrective actions taken, or (3) identify the vulnerabilities discovered and provide a documented basis that justifies actions not taken.

2. For each postulated accident in the design basis occurring in conjunction with each single postulated common-mode failure, the plant response calculated using best-estimate (realistic assumptions) analyses should not result in radiation release exceeding the 10 CFR 100 guideline values, violation of the integrity of the primary coolant pressure boundary, or violation of the integrity of the containment (i.e., exceeding coolant system or containment design limits). The applicant/licensee should either (1) demonstrate that sufficient diversity exists to achieve these goals, or (2) identify the vulnerabilities discovered and the corrective actions taken, or (3) identify the vulnerabilities discovered and provide a documented basis that justifies actions not taken.

3. When a failure of a common element or signal source shared between the control system and the RTS is postulated, and (1) this common-mode failure results in a plant response that requires reactor trip, and (2) the common-mode failure also impairs the trip function, then diverse means that are not subject to or failed by the postulated failure should be provided to perform the RTS function. The diverse means should ensure that the plant response calculated using best-estimate (realistic assumptions) analyses does not result in radiation release exceeding 10% of the 10 CFR 100 guideline value, or violation of the integrity of the primary coolant pressure boundary.

4. No failure of monitoring or display systems should influence the functioning of the RTS or the ESFAS. If plant monitoring system failure induces operators to attempt to operate the plant outside safety limits or in violation of the limiting conditions of operation, the analysis should demonstrate that such operator-induced transients will be compensated by protection system function.

The above result (that all of the BTP HICB-19 acceptance criteria are met) is assured by the TXS D-in-D&D. That is, since there is no common-mode failure that can completely disable the RTS and/or ESFAS, continued sufficient availability of these systems (with a common-mode failure) means that the current licensing-basis acceptance criteria for all FSAR/USAR analyzed events continue to be met. These acceptance criteria are more

conservative than (and thus bound) the acceptance criteria allowed per BTP HICB-19, since the latter assumes a best-estimate approach.

[

] TXS design measures used for error avoidance and fault tolerance will be extremely effective at both preventing and minimizing the consequences of the highly unlikely TXS failure due to an unknown cause. Diversity is enhanced through the skillful application of both safety and non-safety related I&C Systems using both the TXS and TXP systems.

Indicators and alarms for events requiring operator manual action are provided by highly reliable components that operate independently from the TXS software. Should an event occur, these indicators and alarms will be available to alert the operator so that operator action for most events can be taken in accordance with plant procedures.

In conclusion, each protection or mitigation function credited in the safety analyses described above remains available from TXS with the same degree or better reliability as the original analog RTS and ESFAS. All the events described above continue to meet established FSAR/USAR acceptance criteria with equivalent protection or mitigation functions provided by TXS.

It should also be noted that, as described in other sections of this report, the design, qualification, and in-service testing afforded by the FANP TXS system minimize the probability of failures of all types. Moreover, the digital I&C system is designed so that challenges to the safety I&C systems occur at a significantly low rate. Interdependence between the proposed RPS and other support systems has been considered, including the requirements of the ATWS Rule, i.e., 10 CFR 50.62 (Reference /15/). In this area, special attention has been given to diversity between AMSAC and the proposed digital RPS. The upgraded design will thus continue to meet the requirements of the ATWS Rule.

9 CONCLUSION

The methodology used by AmerenUE, WCNOC, and FANP for implementing the FANP TXS digital computer-based RPS is based on a three-pronged approach. Safety is achieved through:

- Dependability (Quality, Testability, and Reliability),
- Diversity, and
- Defense-In-Depth.

This D-in-D&D strategy has been devised to satisfy NRC acceptance criteria while achieving three primary implementation goals:

- To minimize the addition of new diverse indications or automatic controls. With judicious arrangement of I&C equipment, it is possible to preserve the integrity of signals to control systems and PAMS indications, even in the presence of implausible software common-mode failure. This ensures that the information available to the operator remains sufficient to place and maintain the plant in a hot-shutdown condition.

- To minimize the addition of new manual controls and operator actions. This ensures that existing operating procedures remain largely sufficient to address the possibility of software common-mode failure. Meeting this goal also minimizes additional training requirements for operators.

- To implement the new system within the bounds of existing safety analysis and design basis assumptions without the need for extensive new FSAR/USAR Chapter 15 accident analysis. Under these conditions, best-estimate methods are adequate to perform an assessment of D-in-D&D.

Insofar as D-in-D&D is concerned, the design, qualification, and in-service testing afforded by the FANP TXS system preclude the probability of failures of all types. Moreover, Callaway Plant and WCGS will be designed so that challenges to the safety I&C systems occur at a significantly low rate. Interdependence between the proposed control systems, RTS, ESFAS, and other support systems has been considered including the ATWS Rule per 10 CFR 50.62 (Reference /15/). In this area, special attention has been given to diversity between the AMSAC and the proposed RPS. The upgraded design will continue to meet the requirements of the ATWS Rule.

The report described ten features used in the design of the TXS system. These features use simple concepts that when combined prevent system-level software common-mode failure from defeating safety functions. [

] Additional provisions are provided to validate and prevent the propagation of faulty data between channels so only reliable high quality data is used. Watchdog timers are used that place the system in a known predefined condition if a hardware or software exception occurs that results in CPU failure. Systems providing defense-in-depth for plant controls and monitoring and indications used to take operator action are built to be both diverse and independent from TXS software. TXS design measures used for error avoidance and fault tolerance are extremely effective at precluding postulated software common-mode failures. Diversity is enhanced through the skillful application of both safety and non-safety related I&C Systems using both the TXS and TXP systems.

A second line of defense-in-depth is provided by AMSAC and controls for manual actuation. These systems are also built diverse and independent from TXS. Even though software common-mode failure of the RTS, ESFAS, and other TXS safety systems is considered implausible, the TXS architecture has been carefully designed to assure that the control systems, AMSAC, and indications necessary for operator action remain available, even if two software common-mode failures are postulated. Indicators and alarms for events requiring operator manual action are provided by highly reliable components that operate independently from the TXS software. Should an event occur, these indicators and alarms will be available to alert the operator so that timely and appropriate operator action can be taken in accordance with plant procedures.

Transients and accidents continue to meet NRC acceptance criteria for their postulated events and continue to demonstrate adequate diversity. The assessment for these events concluded that even with a postulated software common-mode failure, the required safety function is always available. The overall results of the D-in-D&D Assessment described in this report are summarized in Section 8, "Spectrum of Transients and Accidents."

In conclusion, each protection or mitigation function credited in the safety analyses remains available from TXS with the same degree or better reliability as the original analog RTS and ESFAS. All the FSAR/USAR events continue to meet established acceptance criteria with equivalent protection or mitigation functions provided by TXS. Goals and objectives to preserve the safety integrity of the plant without adding new automatic controls and additional diverse systems are achieved while meeting NRC acceptance criteria. The methods chosen simplify the long-term replacement of systems while maintaining resemblance and integrity of the original plant. Building diversity within the design of each individual TXS system provides the added advantage that each proposed system replacement can be implemented and tested independent of other proposed system upgrades and minimizes the need for additional operator training for responding to abnormal operational occurrences, accidents, and transients.