



UNITED STATES
NUCLEAR REGULATORY COMMISSION

WASHINGTON, D.C. 20555-0001

May 5, 2000

Mr. James F. Mallay
Director, Nuclear Regulatory Affairs
Siemens Power Corporation
2101 Horn Rapids Road
Richland, WA 99352

SUBJECT: ACCEPTANCE FOR REFERENCING OF LICENSING TOPICAL REPORT
EMF-2110(NP), REVISION 1, "TELEPERM XS: A DIGITAL REACTOR
PROTECTION SYSTEM" (TAC NO. MA1983)

Dear Mr. Mallay:

The NRC staff has completed its review of Topical Report EMF-2110(NP), Revision 1, "TELEPERM XS: A Digital Reactor Protection System," submitted by Siemens Power Corporation (SPC) on September 1, 1999. Revision 0 of the topical report was submitted on September 23, 1998, and Revision 1 incorporated the resolution of all comments received from the NRC on the review of Revision 0.

On the basis of our review, the staff finds the subject report to be acceptable for referencing in license applications to the extent specified, and under the limitations delineated in the report, and in the enclosed safety evaluation (SE). The SE defines the basis for NRC acceptance of the report.

Pursuant to 10 CFR 2.790, we have determined that the enclosed SE does not contain proprietary information. However, we will delay placing the SE in the public document room for a period of ten (10) working days from the date of this letter to provide you with the opportunity to comment on the proprietary aspects only. If you believe that any information in the enclosure is proprietary, please identify such information line by line and define the basis pursuant to the criteria of 10 CFR 2.790.

The staff will not repeat its review and acceptance of the matters described in the report, when the report appears as a reference in license applications, except to assure that the material presented is applicable to specific plant involved. Our acceptance applies only to the matters described in the report.

In accordance with the procedures established in NUREG-0390, the NRC requests that SPC publish accepted versions of the report, including the safety evaluation, in the proprietary and non-proprietary forms within 3 months of receipt of this letter. The accepted versions shall incorporate this letter and the enclosed evaluation between the title page and the abstract. The accepted versions shall include an "-A" (designating accepted) following the report identification symbol. The accepted versions shall also incorporate all communications between SPC and the staff during this review.

James F. Mallay

- 2 -

May 5, 2000

Should our criteria or regulations change so that our conclusions as to the acceptability of the report are no longer valid, SPC and the licensees referencing the topical report will be expected to revise and resubmit their respective documentation, or to submit justification for the continued effective applicability of the topical report without revision of their respective documentation.

Sincerely,

/RA/
Stuart A. Richards, Director
Project Directorate IV and Decommissioning
Division of Licensing Project Management
Office of Nuclear Reactor Regulation

Project No. 702

Enclosure: Safety Evaluation

DISTRIBUTION:

PUBLIC

PDIV-2 Reading

SRichards (RidsNrrDlpmLpdiv)

JCalvo

EPeyton (RidsNrrLAEPeyton)

NKalyanam (RidsNrrPMNKalyanam)

** Used SE as written
*See previous concurrence

OFFICE	PDIV-1/PM	PDIV-2/LA	EEIB	PDIV-2/SC	PDIV/D
NAME	NKalyanam*	EPeyton	JCalvo**	SDembek	SRichards 
DATE	04/26/00	04/26/00		05/02/00	5/4/00

DOCUMENT NAME: G:\PDIV-2\Siemens\MA1983-SER.wpd
OFFICIAL RECORD COPY



UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D.C. 20555-0001

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

SUMMARY

This safety evaluation provides the results of the NRC staff's review of Topical Report EMF-2110 (NP), Revision 1, "TELEPERM XS: A Digital Reactor Protection System" and accompanying proprietary documents. The staff also audited the TELEPERM XS (TXS) design implementation and associated documentation at the Siemens' office in Erlangen, Germany, in December 1999, and the results of the audit are also included in this safety evaluation. Based on the information provided and the review conducted, the staff concludes that the design of the TXS system is acceptable for safety-related instrumentation and control (I&C) applications and meets the relevant regulatory requirements.

The TXS system is a distributed, redundant computer system. It consists of three or four independent redundant data-processing automatic paths (channels), each with two or three layers of operation and running asynchronous with respect to each other. Layers of operation include signal acquisition, data processing, and actuation signal voting. In addition to the computers associated with the automatic paths, there are two redundant message and service interface computers to interface with each channel. The design provides for manual trip capability at the system, and component level, independent of the TXS system computers. Isolation and interaction between Class 1E and Non-Class 1E equipment is accomplished through end-to-end fiber optic cables found acceptable in previous license applications in the United States.

The TXS system architecture basic building blocks can be grouped into four categories:

1. System hardware - The TXS selected hardware platform uses a processing computer module, which includes random access memory for the execution of programs; flash erasable programmable read only memory for storing program code; and electrical erasable programmable read only memory for storing application program data.
2. System software - The TXS consists of a set of quality-controlled software components. The execution of the software centers around the operating software system which was developed by Siemens, specifically for the TXS systems. The operating system communicates with the platform software, and application software. The platform software includes the runtime environment program that provides a unified environment for execution of the function diagram modules.

3. Application software - The application software performs the plant-specific TXS safety-related functions using function block modules which are grouped into function diagram modules. The application software is generated by SPACE tools which use the qualified software modules from the function block library to construct a specific application.
4. SPACE tool - The SPACE (specification and coding environment) tool is an engineering system that is used to implement the requirements of plant-specific I&C features.

The German nuclear licensing authority contracted with the German Reactor Safety Association (GRS) to perform product certification. The GRS contracted with two German organizations to review, inspect, and certify products associated with the TXS system equipment and software.

The TXS system equipment qualification, and software verification and validation included temperature and humidity tests, seismic tests, electro-magnetic interference/ radio frequency interference qualification, and software type testing.

Equipment qualification was performed through type testing according to German safety standards which were compared by the staff against the U.S. nuclear industry equipment qualification standards. Except for minor deviations between German and U.S. standards, the equipment qualification design was considered to be acceptable. These deviations will be resolved by Siemens and evaluated by NRC during the review of plant-specific applications.

The process for independent verification and validation (IV&V) of the software is consistent with the IV&V process followed in U.S. standards.

The Siemens development process for the software was audited by the NRC staff at the vendor site. The NRC staff conducted a life cycle process audit of the TXS by tracing selected requirements through the software life cycle.

The design principle for software of Class 1E systems is to ensure that the sequence of processing executed for each expected situation can be deterministically established. It discourages the use of non-deterministic data communications, non-deterministic computations, multitasking, dynamic scheduling, use of non-deterministic interrupts and event driven designs. Based on its review, the NRC staff determined the design of the TXS system satisfies this design principle for Class 1E system software.

Concern with common-mode failures in digital systems and defense-in-depth were the subject of SECY-91-292 and positions addressing those concerns were established and documented in the Standard Review Plan (SRP) Chapter 7, Branch Technical Position (BTP) HICB-19. BTP HICB-19 set forth two principle factors for defense against common-mode/common-cause failures: quality and diversity. Maintaining high quality increases the reliability of both individual components and complete systems. The NRC staff has reviewed the TXS qualification and software development life cycle process and determined that TXS has the required quality.

In regard to defense-in-depth and diversity (D-in-D&D), the NRC staff has established acceptance guidelines for D-in-D&D assessment and has identified four echelons of defense against common-mode failures: control systems, reactor trip system, engineered safety feature actuation system, and monitoring and indication system. These guidelines are presented in

BTP HICB-19. The generic methodology proposed by Siemens follows the guidance in BTP HICB-19. Applications following this methodology for a plant-specific D-in-D&D assessment should be found acceptable in this area.

The TXS design is intended to provide a qualified generic digital I&C platform that meets the regulatory requirements and that can be used for a wide range of plant-specific applications. When using this platform for any plant-specific application, the licensee or applicant will need to verify that the qualification details in this topical report meet the plant license requirements. Because this topical report is for a generic platform, licensees referencing this topical report will need to document the details regarding the use of TXS design in plant-specific applications and address all plant-specific interface items including, but not limited to, those listed in Section 6.0 of this safety evaluation.

1.0 INTRODUCTION

By letter dated September 23, 1998, Siemens Power Corporation (Siemens) submitted non-proprietary Topical Report EMF-2110(NP), "Topical Report for the Generic Approval of TELEPERM XS Equipment at the United States Nuclear Regulatory Commission," for staff review. By letter dated September 1, 1999, Siemens submitted Revision 1 of non-proprietary topical report EMF-2110(NP), for staff review, changing the title of the topical report to "TELEPERM XS: A Digital Reactor Protection System." Revision 1 included major editorial and format changes focusing on regulatory aspects described in the U.S. NRC Standard Review Plan (SRP), NUREG-0800, Chapter 7, "Instrumentation and Controls," Revision 4, June 1997.

The TXS is a digital I&C system designed to be used in safety-related I&C applications in nuclear power plants as replacements for or upgrades to analog I&C systems. Typical applications include the reactor protection functions and the engineered safety features (ESF) functions. The non-proprietary topical report EMF-2110 (NP) describes the TXS hardware and software design, qualification testing, and application capabilities. In addition, Siemens submitted the following proprietary documents:

1. Letter NRC:99:037, dated September 1, 1999, "Supporting Documentation for Review of EMF-2110 (NP) Revision 1, TELEPERM XS: A Digital Reactor Protection System"
2. Letter NRC:99:052, dated December 16, 1999, "ERPI and QA Documentation Supporting Review of EMF-2110(NP) Revision 1, TELEPERM XS: A Digital Reactor Protection System"
3. Letter NRC:99:056, dated December 28, 1999, "Additional Information in Support of the TELEPERM XS Review"
4. Letter NRC:00:004, dated January 13, 2000, "Additional Information in Support of the TXS Review"
5. Letter NRC:00:007, dated January 19, 2000, "Additional Information in Support of the TXS Review"

6. Letter NRC:00:008, dated January 25, 2000, "Clarification of Selected Design Aspects of the TXS System"
7. Meeting presentation view graphs dated October 14 and 15, 1999
8. Meeting presentation view graphs dated November 16, 17, and 18, 1999
9. Letter NRC:00:017, dated March 3, 2000, "Clarification of EMF-2341(P), Generic Strategy for Periodic Surveillance Testing of TXS System in U.S. Nuclear Generating Stations"

These documents provide additional information to support the review of the design details of the TXS system. The staff's review of this topical report is generic. Some plant-specific review items that are not addressed in this topical report will need to be addressed and resolved during a plant-specific application review. Those plant-specific items are identified in Section 6.0 of this report.

This safety evaluation follows the guidance of the U.S. NRC Standard Review Plan (SRP), NUREG-0800, Chapter 7, "Instrumentation and Controls," Revision 4, June 1997. Chapter 7 provides guidance to the staff on reviewing complete nuclear power plant designs of the I&C systems. Revision 4 to SRP Chapter 7 also includes review criteria for digital systems.

2.0 SYSTEM DESCRIPTION

TXS is a distributed, redundant computer system. It consists of three or four independent redundant data-processing paths (channels), each with two or three layers of operation and running asynchronous with respect to each other. Layers of operation include signal acquisition, data-processing, and actuation signal voting. The communication between redundant channels uses end-to-end fiber optic cable connections.

The signal acquisition layer in each channel acquires analog and binary input signals from sensors in the plant (such as for temperature, pressure, and level measurements). Each signal acquisition computer distributes its acquired and preprocessed input signals to the data-processing computers in the next layer. Thus, each data-processing computer is provided with the same set of input information.

The data-processing computers perform signal processing for plant protective functions such as signal online validation, limit value monitoring and closed-loop control calculations. The data-processing computers then send their outputs to two independent voter computer units.

The signal on-line validation uses a 2nd minimum (or 2nd maximum) principle. For a redundant measurement system, each protection channel uses the 2nd lowest measurement to compare the low setpoint value and then determines the partial trip status of that channel for a "low trip" parameter. Similarly, it uses 2nd highest measurement to compare the high setpoint value and then determines the partial trip status of that channel for a "high trip" parameter. This method will reject the outlying signal in the process measurement and thereby minimize inadvertent trips.

In the voter computers, the outputs of the data-processing computers of redundant (three or four) channels are processed together. A voter computer controls a set of actuators. Each voter receives the actuation signal from each of the redundant data-processing computers. The voter's task is to compare this redundant information and compute a validated (voted) actuating signal, which is used for actuating the end devices.

The actuation logic employs either a TXS relay voter or a TXS digital voter. The reactor trip signals are voted by relay voters and the ESF actuation signals are voted by TXS digital voters, or TXS relay voters depend on the plant ESF system interface condition. The TXS relay voter votes 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. For each relay an additional contact is wired to the TXS monitoring and service interface (MSI) as a relay check-back signal. This is used for test and monitoring purposes. The digital voter performs 2-out-of-4 logic voting of the actuation signals from the processing computers. Each train has two voter computers.

Each TXS digital voter uses a pair of master-checkers in the voting logic to ensure there are no spurious actuations of safety-related equipment. Each master-checker set consists of redundant processors that process the same input signals. The results of the processing are compared, and differences in the results are flagged as possible errors in the processing that developed the voter input signal or in one of the processors that performed the voting operation. Since the master-checker redundant processors must use the same input data, the processors run synchronously, unlike the asynchronous processor operations between any two of the characteristic four channels of safety functions. If the processor outputs do not agree, the master-checker pair selects the default fault state, in which the output signals are set to 0 and the load power supply is disconnected. This use of the master-checker pair ensures that failures of a processor will not result in a spurious initiation of a safety function and that a master or checker processor will not disable the protection function in that channel.

For fail-safe and fault-tolerant outputs to the reactor switchgear, the TXS uses a voter configuration. The voter configuration consists of two sets of master-checker pairs in each channel, with a separate power supply. This configuration ensures that random signal failures only affect one half of a voter. Because the output signal of the two halves of the voter are applied to a hardware "OR" element, the second half of the voter assumes control of the switchgear in the event of such a failure. Both master-checker pairs in the two halves of the voter and interaction of the halves of the voter operate synchronously. The voter configuration ensures that single failures can result neither in spurious signals nor in loss of function.

In addition to the computers of the above-described automatic path, there are two redundant MSI computers to interface with each channel. The MSI computers are connected to each automatic path and to its assigned voters. The MSI serves as a gateway between the computers of the automatic path and other non-safety-related systems such as service units, process control computers, and monitoring computers. Either MSI unit can perform interfacing and diagnostic functions. The safety protection system signal passes through the MSI to display information at the main control board. The non-safety-related service unit requests access through the MSI to perform the diagnostic function at the safety-related processor. The service unit can be implemented as a single computer system or as a distributed system with several workstation computers. It can be installed temporarily or permanently. Parallel operation of several workplaces is possible.

The service unit contains the central data of the I&C system. It is the central means for interventions into the safety-relevant software of the function processors. The test machine for conducting periodic surveillance testing of the I&C system has a bus interface with the service unit. The software for the test machine operates as a client of the service unit. The service unit is protected against unauthorized interventions. The control mechanisms are installed by software so that only authorized persons may access the service unit, only authorized interventions may be performed, and interventions are restricted to a single redundant channel at a time. All signaling messages cyclically transferred by the service unit are recorded, checked for changes, and archived by the service monitor assigned to the service unit computers.

Manual reactor trip capability is provided on a per train basis. The manual trip signal at the system level totally bypasses the TXS processing and voting computers. Manual controls of safety actuators also bypass the TXS processing units and go directly to individual components via the priority logic which is located in the output of the voting units for the ESF actuation systems, and via the relay logic, which is independent of the voting computers, for the reactor trip system.

The TXS system architecture basic building blocks can be grouped into four categories:

1. SPACE tools - The SPACE tool is an engineering system that is used to implement the requirements of plant-specific I&C features.
2. System software
3. System hardware:
 - a. Hardware structure including backplane bus
 - b. Processing modules
 - c. Communication systems
 - d. I/O modules
4. Application software - The application software is generated by SPACE tools which use the qualified software modules from the function block library to construct a specific application. The programs will be stored in FEPRM (flash erasable programmable read only memory).

To create a specific application project, the first step is to define the hardware specification, which contains the complete hardware structure of the target system with all of its components. The hardware specification is created using the SPACE editor. The SPACE editor is a graphical user interface tool to create I&C function diagrams and hardware diagrams. Each function diagram is assigned to one processing module, on which it is processed. This assignment is done while creating the hardware diagrams. The information is stored in the specification database.

SPACE code generators are used to interpret the contents of the specification database and to automatically generate high-level language code (in C language) for each function diagram. Communication between function diagrams is done using data messages. These are also automatically generated by interpreting the hardware specification and the software-hardware

assignment. Thus the complete code for all function diagrams is automatically generated. Automatic code generation reduces the probability of coding errors and reduces coding time. Independent tools are developed to perform automatic code verification. The SPACE tools parse the generated code, transform it into an internal representation, and compare this representation to the information stored in the specification database.

Specific communication methods are applied to ensure interference-free communication inside the TXS system and within the plant process information system. The TXS design requires that in case of a single failure of one of the independent processing channels or within one communication path in the same processing channel, the channels still available will continue to operate as designed on the basis of the remaining information to ensure the required safety functions do not fail. The communication from the safety I&C system to the plant process information system is done via the MSI computer as previously explained. This communication channel is used by signaling messages to the plant process system. The MSI serves as a means of isolation within the TXS architecture. The link through the MSI gateway computer is configured so that the faults in the non-safety-related I&C systems cannot affect the operation of the safety-related I&C system.

An important aspect of the system software is the functioning of the runtime environment (RTE) which is essential for the TXS communication. The internal system clock (every millisecond) triggers and controls all actions during the processing cycle. The central control unit sequentially starts the main processing phases in each processing cycle (typical cycle time is 50 ms). A typical real-time processing cycle starts in the following sequence:

1. Reading input data,
2. Input checks of received messages,
3. Processing application software,
4. Handling of transmitted messages,
5. Transferring the output messages,
6. Processing of diagnostic programs for the remaining processing cycle time, and
7. Processing self monitoring programs.

The TXS CPU features a hardware watchdog timer which has an independent clock. This watchdog is triggered by the cyclic task of the RTE. On the beginning of each computing cycle the watchdog timer is set. If the watchdog is not triggered by the RTE in time, it times out and activates the exception handler. Thus, the hardware watchdog monitors the RTE cyclic task.

The RTE includes a feature that monitors the internal counter of the cyclic self-monitoring task. The cyclic self-monitoring function keeps an internal counter, which is incremented once in every complete cycle of the cyclic self-monitoring. This timer is triggered by the self-monitoring task when the cycle is started. If this counter has not been changed (incremented) within a specified period of time, the RTE issues an error message. The time needed for a complete cycle of self-monitoring depends on the CPU load. When more of the cycle time is used by application software, less time is available for cyclic self-monitoring. However, the complete cycle is typically carried out in 300 to 600 seconds.

The detailed hardware and software descriptions are discussed in Sections 2.1 and 2.2 of this safety evaluation.

2.1 Hardware Description

The TXS-selected hardware platform uses a processing module, which includes Random Access Memory (RAM), Flash Erasable Programmable Read Only Memory (FEPRM) for storing program code, and Electrical Erasable Programmable Read Only Memory (EEPROM) for storing application program data. Input and output modules are standard components designed for an automation system; these modules have been in service in other technological fields for many years and in many applications. Communication processing modules are available for the Local Area Network (LAN) standard Ethernet and Profibus (process field bus). These boards are mounted in racks and communicate via a 32-bit multi-master-capable parallel backplane bus. Other LAN components such as electrical-to-optical transducers and star coupler components are also industry standard components.

The hardware-associated interrupts are the following:

Time 0 interrupt: This interrupt is generated by a hardware timer once every 1 ms. It is used as the operating system's time interrupt. This interrupt is handled by the MICROS operating system. The interrupt service routine increments the internal operating system time by 1. Then, it enters the scheduler and resumes the execution of the task previously interrupted which is normally associated with an application program phase under the control of the processing cycle, unless the application program cyclic task has completed. All the safety-related application programs are assigned the same high priority to ensure that once the execution of a program starts, it goes to completion without being interrupted by another application program. The only task assigned higher priority than the application program is the MicroNet Interrupt Service task which can only be activated by the LBUS hardware interrupt. The LBUS hardware interrupt does not occur during normal operation.

K32 backplane bus interrupt (IRE): This interrupt is generated by another CPU via a memory mapped write access. If a CPU writes to a certain memory address, an IRE interrupt can be generated on another CPU. The IRE interrupt is handled by the MICROS operating system. It is configured so that MICROS will start a predetermined task when the IRE occurs. This interrupt is used in TXS in two cases:

1. If a CPU wants to send data via a communication processor, this CPU initiates an IRE interrupt on the communication processor. The IRE activates a task on the communication processor, which then looks for new data to be sent and sends them via its network interface. Using this technique, the time delay on the communication processor is minimized. The sending of data is a periodic process controlled by the RTE's cycle task.
2. The IRE is also used on voter master/checker pairs. Here the IRE is used to start the checker's cyclic task, thus ensuring synchronous operation of master and checker. This works in the following way: On the master, the RTE's cyclic task is started by the MICROS operating system based on the operating system's time (for example every 50 ms). Once the master's cyclic task is running, one of its first actions is to send dummy data to his checker via the backplane bus initiating an IRE interrupt on the checker. The data are not relevant here, they are only sent to initiate the IRE on the checker. On the checker, the IRE is handled by the MICROS operating system, which is configured in a way that the checker's RTE cycle task will be activated. The master's RTE cycle task is

started periodically (typically every 50 ms). Likewise, the IRE on the checker will occur with the same frequency.

LBUS interrupt: This interrupt can be generated by subsystems connected to the processing module (SVE1) local extension bus (LBUS). It is generated by a subsystem when it is reset or powered up. This interrupt is handled by the MICROS operating system. When it occurs, MICROS starts a task which notifies the communication software MicroNET, that a subsystem has restarted. By this method, MicroNET is able to re-establish the communication channels to communication partners in this subsystem (if any). This interrupt can only occur if subsystems are connected to the SVE1 processor. Even in this case, the interrupt only occurs when the subsystem is reset or powered up, which is not the case during normal operation.

LAX-module interrupt: This interrupt is generated by the LAX-module (Ethernet interface board) of the communication processor (SCP1). The interrupt is generated by the Ethernet controller on the LAX board when a frame is received from the Ethernet network. The interrupt is handled by the SCP1 protocol handler firmware. This interrupt is only used on the SCP1 communication processors.

All other interrupts are either disabled or do not occur during normal operation. All of these hardware interrupts have been designed for strictly deterministic behavior.

2.1.1 Physical Description

TXS hardware basically consists of four types of components: the subracks, function processors, communication modules, and input/output (I/O) modules. These basic components can be configured to constitute a digital safety I&C system to replace an existing analog safety I&C system. The new configured digital safety I&C system may be located in same place as the existing cabinet and may utilize the existing field cables for input and output signals. The existing channel separation will be maintained.

Subrack

The subrack contains the electronic printed-circuit boards (PCBs). Cooling fans are energized with Class 1E power. Fan operation is monitored and fan failures resulting in an excessive temperature inside the cabinet will be monitored and alarmed. The subrack is equipped to cool the modules and protects them from electromagnetic interference.

Function Processor

The function processor module is the application programmable module for executing the safety functions. The I&C functions are stored as executable programs in the write-protected FEPRM along with the necessary system functions, and are validated by cyclic redundancy checks (CRCs). An executable program is a sequence of executable commands executed by the CPU. All components of a function processor are always used in the same way and in a recurring sequence. Data and programs that are required to implement I&C functions are permanently assigned to defined memory locations in advance.

The input signals for I&C functions that are implemented on a function processor are provided either in the form of messages via the MSI or as single-wire signals via I/O modules. Similarly,

the output signals of the I&C functions are passed on either as messages or as single-wire signals. Signals from the I/O module are read by the function processor from the data buffers of the I/O modules via the backplane bus or written to the data buffers. Data exchange with the MSI passes through the dual-port RAMs. Physically different areas of the dual-port RAM are dedicated to receiving and sending data.

Communication Modules

Communication is based on serial buses. Data transmission is performed in the following steps:

- The function processor writes the data to be transmitted into the dual-port RAM of the interface module.
- The data are serially transmitted via the network to the interface module of the destination system in accordance with protocol used.
- The interface module transmits the data to the dual-port RAM of the destination function processor.
- The destination function processor reads the data and checks the data integrity.

Input/Output Modules

All modules are plug-in PCBs. Analog modules contain an analog-to-digital or digital-to-analog converter and a multiplexer. Each module is capable of handling eight input variables. Digital modules can handle 32 inputs. The analog input data is stored in dedicated memory locations for each input. This data is read by the function processor. The digital input data is directly read by the function processor from the digital module.

2.1.2 Product Qualification

Equipment qualification was performed through type-testing according to German safety standard KTA-3503, "Type Testing of Electrical Modules for the Reactor Protection System." The hardware type tests began in 1993 and ended for the first set of hardware modules in 1996. The results of the type tests were documented by certificates and associated evaluation reports. Each qualified component has its own certification and its own evaluation report. If a certified product requires a modification, the modified product is required to have a new certification.

The German nuclear licensing authority contracted with the GRS to perform product certification. The GRS contracted with the German Technical Inspection Agency (TÜV, Technischer Überwachungs Verein) to review, inspect and certify products. The TÜV verifies the consistency of the design documents and the requirements specified in the safety-related applications. The TÜV also inspects the design process and test results. In some cases TÜV may perform independent tests to verify the performance of a product. When TÜV completes its review, it issues a product certification. The certified product can be used for subsequent applications.

The equipment qualification tests were performed in the following test sequence:

1. Visual inspections,
2. Functional tests,
3. Test of electrical characteristics,
4. Climatic tests (including temperature and moisture tests),
5. Test to demonstrate the electromagnetic compatibility conditions,
6. Mechanical stress tests (including seismic qualification test), and
7. Another functional test to verify no degradation of function.

The TXS system was developed in several stages. Qualification was implemented in four steps:

Step 1: The conceptual design was reviewed by GRS and TÜV, and the design was accepted in 1992.

Step 2: The following hardware components were type tested:

- Components for signal processing,
- Components for communication,
- Components for input and output of digital and analog signals, and
- Subracks and electrical accessories.

Third-party assessment of hardware type testing was completed in 1998. The test results were summarized in two test reports:

- (1) "Summary Test Report for Type Test of Modules in TXS," TÜV Nord, March 18, 1998.
- (2) "Documentation of the Practical Test - Overview of Test Documentation - Summary of Test Results of the TXS System," TÜV Rheinland, March 18, 1998.

Step 3: Type testing of software includes the following:

- The runtime environment,
- The function diagram group modules, and
- The function block modules.

The test procedure was closely linked to the different stages of software development. GRS was contracted to perform the third-party assessment for software type testing. The assessment began in 1992 and was finished in 1997.

Step 4: Quality verification of the program development tools for integrating the platform with plant specific application programs (such as SPACE system) was included in the software type testing. The quality verification confirmed that the tools are functionally and qualitatively suitable for performing their tasks. Quality verification was completed in 1997.

The staff requested that Siemens provide a comparison between the German type testing standard and the U.S. nuclear industry equipment qualification standards. By letter NRC:00:007 dated January 19, 2000, Siemens submitted report EMF-2352(NP), "TXS Qualification Testing." Elements of the TXS qualification testing program were evaluated against the requirements and acceptance criteria identified in the Electric Power Research Institute (EPRI) report TR-107330, "Generic Requirements Specification for Qualifying a Commercially Available PLC (programmable logic controller) for Safety-Related Application in Nuclear Power Plants," for seismic and environmental qualifications. The results of this assessment are summarized below.

Seismic Qualification Testing

Applicable Standards:

- IEEE Standard 344-1975
- EPRI TR-107330, Figure 4.5

Acceptance Criteria:

EPRI TR-107330, Section 4.3.9

The I&C system shall operate as intended for the specified level of vibration. All connections in the system shall remain intact, all modules shall remain fully inserted, and no functional or non-functional parts shall fall off their specified levels. If relay output modules are included for qualification, then the relay contacts shall be capable of changing state from energized to de-energized and deenergized to energized during application of the operating basis earthquake (OBE) and the safe shutdown earthquake (SSE). Any spurious change of state shall not exceed 2 milliseconds for both energized and deenergized relays.

Environmental Testing

Applicable Standards:

- EPRI TR-107330, Sections 4.3.6.1, 4.3.6.2, and 4.3.6.3
- EPRI TR-107330, Figure 4-4

Acceptance Criteria:

EPRI TR-107330, Sections 4.3.6.1, 4.3.6.2, 4.3.6.3 and 5.3

The I&C system shall operate for the temperature and humidity environmental profile provided in EPRI TR-107330, Figure 4-4, and the operability requirements stated in Section 5.3.

The seismic and environmental qualification tests performed on the TXS I&C system satisfied the majority of the test requirements specified in EPRI TR-107330. However, some deviations were noted as explained in Sections 2.1.2.1 and 2.1.2.2.

The staff has reviewed the documentation of the practical test results of the TXS system. The purpose of the practical test is to verify that the test objects (TXS modules) meet the

safety-related requirements and regulations specified in KTA-3503 and the requirements specified by the supplier. The tests were performed by TÜV Rheinland and TÜV Nord (both of the German Technical Inspection Agency) from March 1994 through January 1998. The test results were documented in TÜV reports 945/K 72999/98 and TXS-980318-PB, both dated March 18, 1998.

Based on the audit of these reports, the staff found that the TXS system hardware design has complied with German safety standards. However, in order to meet the generic qualification requirements for U.S. nuclear plants, the product should also meet the U.S. testing requirements specified in the EPRI report TR-107330 for the two issues discussed in the following sections. EPRI TR-107330 was approved by the staff on July 30, 1998.

The software qualification findings are presented in Sections 2.2.2.14, 2.2.2.15, and 4.4.

2.1.2.1 Environmental Qualifications (Temperature and Humidity Tests)

A detailed compliance matrix showing the relationship between EPRI requirements and the TXS system design was documented in proprietary report TR-104017, "Siemens TXS Compliance with EPRI TR-107330." As stated in TR-104017, environmental testing was performed on a fully loaded representative TXS system, and the operation was under the control of generic application software. The objective of these tests was to prove the adequacy of the materials and system design under all conditions to which the system might be subjected from factory to final in-service operation. The following tests were performed:

- Steady-state cold with modules not in operation
- Steady-state dry heat with modules not in operation
- Steady-state damp heat with modules not in operation
- Temperature cycle test with modules not in operation
- Cyclical humidity with modules not in operation
- Steady-state damp heat with modules in operation
- Cyclic dry heat with modules in operation

As stated in the TR-104017, comparing the TXS testing condition and the EPRI testing requirements, the TXS tests did not achieve the maximum temperature in the EPRI testing requirements. An environmental qualification retest of the TXS was planned to meet the EPRI requirements. The above tests were performed without the cabinet enclosure. The absence of a cabinet enclosure did not allow for internal cabinet temperature effects and confirmation of the effectiveness of the cooling configuration. The TXS design has a provision to monitor temperature inside the cabinet. The plant-specific application should identify in the plant operating procedures monitoring internal cabinet temperature to ensure that the internal cabinet temperature will be always under the environmental qualification envelope, and develop plant-specific procedures to respond to TXS cabinet/subrack high temperature alarms. This is a plant-specific action item.

2.1.2.2 Seismic Qualification

To demonstrate that the operability of the component is not degraded by mechanical stresses, tests of mechanical stress were performed by Siemens. The seismic qualification test was one of the test procedures in hardware qualification tests. The seismic qualification test was based

on IEEE Standard 344-1987 criteria. The amplitude of acceleration for the test input accounts for the natural frequency (18 Hz), and the magnification factor for the supporting structure (1.56) of the I&C cabinets to be used, as well as the acceleration spectrum for the design of a typical PWR plant. The input excitation used was multiple frequency ranging from 5 to 35 Hz, and 3 axes, each staggered by 90°. Test duration per axis was a minimum of 1 minute. The functioning of the component was monitored during the test. The technical data were not violated. Following the test, a visual inspection and an intermediate functional test were performed. The test results were documented according to IEEE-344, Section 10.

However, as stated in TR-114017, the TXS seismic testing level is below the EPRI requirements. The TXS seismic test level does not completely envelop all U.S. nuclear plants required test levels. In order to be useful for most of the U.S. nuclear plants, a seismic qualification retest for the TXS system was planned to comply with the EPRI seismic testing requirements. A U.S. licensee that uses the TXS system for a safety system application should compare its required seismic qualification level to the Siemens' qualified level, and identify areas requiring further action. This is a plant-specific action item.

2.1.2.3 Electro-Magnetic Interference (EMI) / Radio Frequency Interference (RFI) Qualification

EPRI submitted Topical Report TR-102323, "Guideline for Electromagnetic Interference Testing in Power Plants," for staff review in 1994. The topical report was developed by EPRI to recommend alternatives for performing site-specific electromagnetic interference (EMI) surveys for qualifying digital plant safety instrumentation and control equipment in a plant's electromagnetic (EM) environment. The recommendations in TR-102323 include (1) a set of electromagnetic interference and radio frequency interference (EMI/RFI) susceptibility testing levels, (2) EMI eliminating practices, and (3) equipment EMI/RFI emission testing levels. The above recommendations are based on EMI/RFI emission data collected during 1993 and 1994 at seven nuclear power plants and data collected before 1993 at other nuclear power plant sites.

In 1996, the staff issued a safety evaluation concluding that the TR-102323 recommendations and guidelines provided an adequate method for qualifying digital I&C equipment for a plant's EM environment without the need for plant-specific EMI surveys if the plant-specific EM environment is confirmed to be similar to that identified in TR-102323.

Siemens performed electromagnetic compatibility (EMC) qualification tests on the TXS components as described in the TÜV report TXS-980318-PB, "Documentation of the Practical Test Overview of Test Documentation-Summary of Test Results of TELEPERM XS System," dated March 18, 1998. The results of the EMC qualification tests show that the tested TXS did not satisfy all the test requirements specified in EPRI TR-102323. The main reason that the TXS did not meet all the test requirements specified in EPRI TR-102323 was the difference in the requirements of the European EMC test standard (used by Siemens) and the EPRI TR-102323 specification. Additionally, the configuration of equipment used for the EMC qualification tests might not be the most adverse EMC configuration of the TXS I&C system equipment. To resolve these two issues, Siemens stated that it will perform EMC qualification tests in accordance with EPRI TR-102323 on the most adverse EMC TXS I&C equipment configuration for the EMC qualification tests.

Based on this commitment, the staff finds that the TXS I&C system equipment EMC qualification would be considered acceptable provided that Siemens successfully completes the proposed EMC tests. Additionally, before installing the TXS system as a safety system in a nuclear power plant, a licensee should verify that its plant electromagnetic environment and its TXS system configuration are enveloped by EPRI TR-102323 EMC qualification tests. This is a plant-specific action item.

2.1.2.4 Power Supply Quality Requirements

TXS applications in Europe were designed to operate with a DC power source providing input power to the TXS racks. However, most nuclear power plants in the United States provide an AC power source for Class 1E instrumentation and control systems. For these applications, Siemens will qualify an AC to DC power supply converter that complies with EPRI TR-107330 electrical power supply and qualification requirements. This is a plant-specific action item.

2.1.3 Isolation and Interaction Between Class-1E and Non-Class-1E Equipment

In the TXS system design, signals interact between redundant Class-1E channels and transmit from Class-1E channels to non-Class-1E devices. The communication between Class-1E channels uses end-to-end fiber optic cables found acceptable in previous license applications in the United States. The communication from the safety I&C system to the non-safety plant information system is done via the MSI. The MSI serves as a means of isolation within the TXS architecture. For the upgrade of existing analog instrumentation and control systems in United States nuclear power plants, there is a need to provide an interface between Class-1E and non-Class-1E systems by means of both analog signal and relay contacts. For these applications, Siemens will qualify an analog isolation device and a mechanical relay to provide adequate coil-to-contact isolation. This qualification will be performed in accordance with the class 1E to non-Class-1E isolation requirements of EPRI TR-107330. This is a plant-specific action item.

2.2 Software Description

The TXS is a digital instrumentation and control system for safety-related applications in nuclear power plants. The system provides a framework in which engineers may design and implement plant-specific safety-related applications. Typical applications are closed-loop controls of reactor processes, reactor trip applications, and applications that initiate engineered safety features actuation signals. The TXS consists of a set of quality-controlled software components that are qualified according to the specific requirements of nuclear reactor safety systems. To control and facilitate development efforts, the TXS system includes a specification and coding environment (SPACE) tool for designing and assembling safety-related applications.

The conceptual architecture for a TXS application serves as the functional specification and design of a TXS plant-specific system, and serves as a bridge between the plant-specific system requirements and the resulting system implementation in software code.

The software and data that do not change are stored in the write-protected flash erasable programmable read only memory (EPROM) area of the function computer. Examples of this type of data are the runtime environment, function diagram group modules, and system parameters that do not change over the life of the system application. This data cannot be

changed without first erasing the data stored in the applicable flash EPROM 64 Kb sector, and then rewriting the entire flash EPROM sector. The flash EPROM data, however, may be changed without removing the flash EPROM from the SVE1 processor board. To ensure the application software and invariable data remain unchanged, flash EPROM data integrity is checked by a self-diagnostic routine that calculates the CRC value of each 64Kb sector of the EPROM and compares the result to the CRC value that is stored in each 64 Kb sector of the EPROM with the application software and invariable data.

Data that is subject to change over the nuclear plant fuel cycle are stored redundantly in electrically erasable programmable read only memory (EEPROM). Examples of this type of data include plant system parameters and setpoints that may require changing by the plant operator, programs required for SVE1 (processing module) startup, and the loader for programming the flash EPROM. Unlike the unchanging data and programs that are stored on flash EPROM, data stored in EEPROM may be changed without first erasing all the data stored in a block of memory in the EEPROM. In addition to checking the EEPROM data with a CRC diagnostic routine, this data is also checked using the redundant copies of the stored data.

Data that changes from one processing cycle to the next are stored in the random access memory (RAM). Examples of this data include plant process input data, intermediate results of the system applications, and output data. Data in the RAM may be changed without the special processes used to write data to flash EPROM and EEPROM. The integrity of the RAM used to store data is cyclically checked by a self-diagnostic routine that writes data to each RAM address and then reads the data to ensure the RAM address correctly stores information.

2.2.1 Teleperm XS (TXS) Software Description

The TXS software can be divided into three categories: operating system software, platform software, and application software. The following sections describe the software in these three categories. The components of each layer of the processing system are shown in Figure 1.

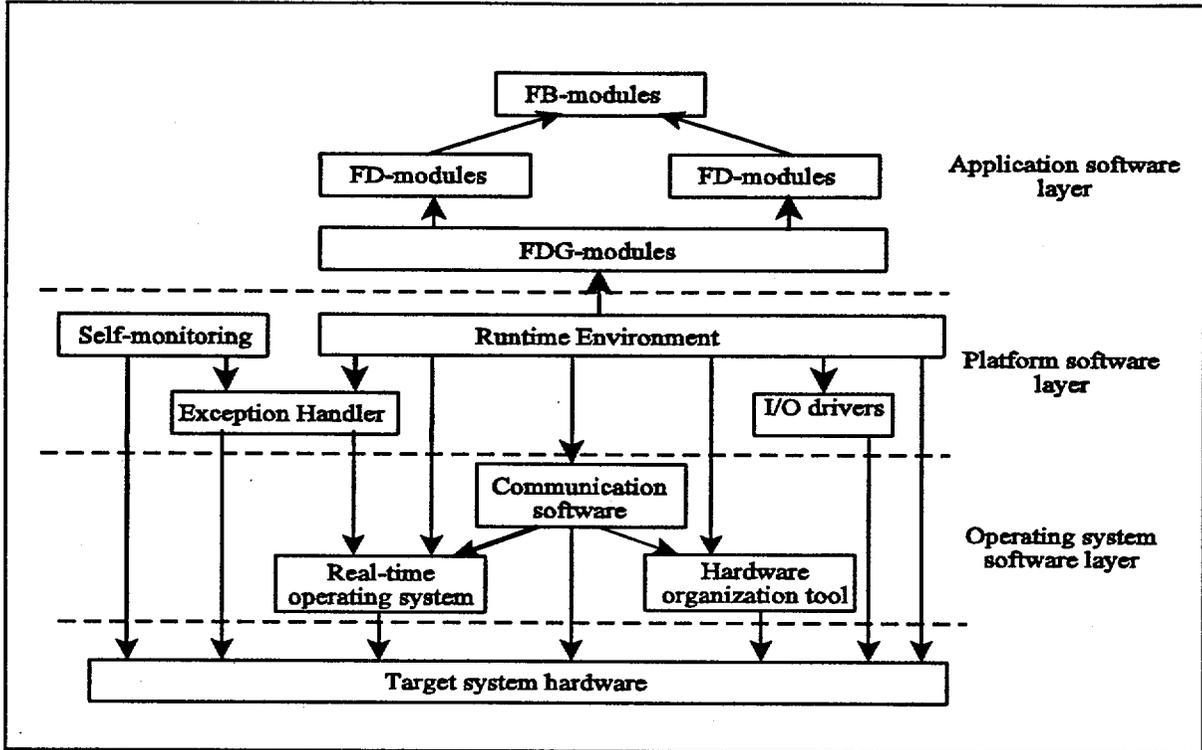


Figure 1. Software layers of one application processor.

2.2.1.1 Operating System Software

The operating system was developed by Siemens Plants and Technical Service Division ATD (Anlagen und Technische Dienstleistungen) specifically for the TXS systems. Development was according to TXS requirements and specifically to International Electrotechnical Commission Standard (IEC-880), "Software for Computers in the Safety Systems of Nuclear Power Stations." Standard IEC-880 is referenced in IEEE Standard 7-4.3.2, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations." IEC-880 is comparable to IEEE Standard 7-4.3.2 and NRC has found Standard IEC-880 acceptable.

The operating system software layer consists of the real-time operating system, communication software, and the hardware organization tool. The components that make up these three categories are summarized in the following discussion.

- MICROS (Real-time Operating System)

MICROS is the real-time operating system kernel of TXS systems. It is small (approximately 1 Kbyte) and static. In this context, the term static means that all the operating system objects are defined on startup and cannot be changed during run time. For example, the operating system does not use dynamic allocation of system resources such as memory-heap or dynamic task definitions.

- NMI-Handler (Real-time Operating System)

The NMI handler, in cooperation with the exception handler, is responsible for handling abnormal conditions. In many cases, hardware failures are signaled by means of interrupts. For example, communication bus accesses to I/O modules are monitored for tolerable response times (time-outs) in this way. If these times are exceeded, it is concluded that a failure has occurred and this is signaled by means of an interrupt. Both the NMI handler and the exception handler are responsible for initiating the required measures in such cases. One important measure involves signaling failure and returning the computer to a predefined state (e.g., disabling of all outputs).

- MicroNET (Communication Software)

MicroNET is responsible for the communication between different function computers, as well as between the communication processors and function computers within the same subrack. MicroNET-L2 is an extension of the communication services that supports L2 (protocol) communication.

- CP486 (Communication Software)

CP486 is the protocol handler implemented in the TXS communication processor. This software module is responsible for transmitting and receiving H1 (communication processor) messages.

- Driver 3964 R (Communication Software)

The 3964R driver constitutes the interface to the local V.24 interface which is used for loading programs and for the output of debug information.

- Hardware Organization Tool

The Hardware Organization Tool (HOT) is responsible for the parameterization of the operating system on computer startup. HOT configures the communication memories and detects whether modules are assigned to the slots in a subrack. The HOT also detects the module types.

In addition to the software modules described above, the TXS operating system provides the following services:

- Debug Services

Debug services support system diagnostic tasks used mainly during the system development and integration.

- Diagnostics Monitor (monitor to support diagnostics)

The diagnostics monitor is a low-level debugging tool. If the computer fails, for example, it is possible to branch to the diagnostics monitor to analyze causes of failure that are difficult to diagnose after the computer has been returned to the defined state (outputs disabled).

Two communication protocols are used in the TXS. Communications between subracks in the same safety channel are via a backplane bus using an H1 protocol (IEEE-802.3). Communications between different channels are over fiber optic connections using the Profibus L2 protocol (DIN 19245). All communications are on serial busses. Data transmission is always performed in the following manner:

- The function processor writes data to be transmitted into the interface module dual-port RAM.
- The data is transmitted via the applicable network and protocol to the interface module of the receiving function processor or system.
- The receiving interface module writes the data into the receiving function processor dual-port RAM.
- The receiving function processor reads the data from its dual-port RAM and checks the data integrity.

Communication between different processors is done by messages. These messages can contain signals from function diagram group (FDG) modules (data messages); control commands from the service unit (control messages); or error messages, trace data, or command responses to the service unit (signaling messages).

Communications cycle between function processors in the same channel and communications between redundant safety channels. That is, each function processor sends one signaling message and receives one command message per processing cycle. Communications via shared dual-port RAM use a handshake protocol: the sender can only send into the channel when it is empty, and the receiver can only read from the channel when it is filled. All messages have an individual, but fixed message length. This ensures that the load on the communication busses is constant and the communications occur in a deterministic manner.

Messages are also transmitted from and to the service unit via the MSI, which organizes the exchange of this information with the function processors. Each MSI can service up to 10 function processors. The cyclic communications are invariant and, therefore, allow the TXS safety system to be fully tested during the system integration phase of the system life cycle.

As discussed above, in addition to communications between subracks in the same safety channel and communications between redundant safety channels, the TXS has communication gateways between the TXS safety channels (through the MSI) and the non-safety-related service unit, plant process control computers, and monitoring computers. Typically the service unit is installed in an electronic or I&C service room near the main control room, and is connected to the TXS MSI via an H1 bus. The gateways are not Class 1E equipment, and are therefore isolated from the Class 1E TXS safety system MSI with optical isolation devices.

Communications between the initiation trains of the safety system and the service unit are cyclic and cannot interrupt the normal functions of the safety system function processors without plant operator intervention. This operator intervention cannot be performed on more than one safety system channel at a time. Interventions of safety system channel operations by

the operator are permitted to change system parameters or tracing signals, to perform periodic tests, and to allow diagnosis of safety system failures.

The TXS RTE controls all processing cycle activities, including communications. The TXS processing cycle is started by the central control unit of the RTE by triggering the internal MicroNet controller to transfer the messages in the receive dual-port RAMs of all linked communication modules into the corresponding message input buffers. After the integrity of the message is checked by means of a 16-bit cyclic redundancy check (CRC) (for the occurrence of random bit errors) and by means of a sequence increment (to ensure that a new message has been received), the message is flagged as a valid or an invalid message for subsequent processing.

The RTE software automatically marks the invalid message and all signals stored in this message with the ERROR status flag. Signals marked with ERROR status flag are excluded from further processing by the function blocks. For example, a "2-out-of-4" voting function block will calculate a "2-out-of-3" function of the remaining 3 input signals, if one input signal is marked with the ERROR status flag. For example, a "2.MAX" analog signal selection block function block will select:

- The "2nd highest" signal of the remaining 3 input signals, if one input signal is marked with ERROR status flag.
- The "2nd highest" signal of the remaining 2 input signals (that means the lower one), if two input signals are marked with ERROR status flag.
- The remaining input signal, if three input signals are marked with ERROR status flag.

Additionally, a communication error flag is set by the RTE. This information is transferred to the service unit and to the main control board alarm system.

The safety function can be postulated to be lost only if all of the incoming data is old or corrupt. For this case a fail-safe state of the function can be designed on the application software level. In all other cases (loss of 1, 2 or 3 input signals) the function will be executed correctly based on a reduced set of available input information. As soon as the communication failure is repaired (that means, the receiving CPU finds new and consistent data in the dual port RAM), the ERROR status for the incoming data will be automatically reset and this data will be used for function processing. No manual initialization is necessary.

During function diagram processing, the valid signals are further processed to determine out-of-range conditions and defective-instrument conditions. All provisional signals are stored in dedicated signal buffers during function diagram processing.

After function diagram processing has been completed, the central control unit triggers the "function diagram group output function" to create output message data from the results of the function group processing. The RTE then adds a message header to the message data, which includes a CRC checksum and the cycle counter, and stores the output message data in the message output buffers.

As the last step in the processing cycle, the RTE triggers the communications control program (MicroNet) to transfer the message data from the output buffers into the sending dual-port RAMs of the respective communication processor. This message data is then sent to other subbracks and the MSI, as required, using either the H1 protocol (within the same channel) or the L2 protocol (between channels).

To achieve a deterministic system behavior, all communication is performed strictly cyclically, with the system-wide unique communication cycle. No event-driven communication is used. Thus, communication loads are constant under all circumstances.

The communication protocols used for sending messages are not acknowledged by the receiver. Thus, the subbrack receiving the message cannot influence the operation of the sending subbrack.

2.2.1.2 Platform Software

The platform software consists of the RTE and its modules, the input/output (I/O) drivers for the input/output module interface, the exception handler, and the self-test software. The purpose of the RTE is to give a unified environment for execution of the function diagram group (FDG) modules. The RTE controls the cyclic processing of the FDG modules and controls signal transfers via messages or directly by I/O modules. The RTE also provides the interface of the runtime system software to an external service unit, through which it can be monitored and controlled (e.g., by signal trace, reading error messages, switching operation modes, and function block (FB) module parameterization).

The RTE provides four operation modes:

- **OPERATION:**

This is the normal operation mode for cyclic processing of the FDG-modules.

- **PARAM:**

This mode is the same as the OPERATION mode, but parameterization of FB-modules and definition of trace data are now allowed.

- **TEST:**

This mode is used for functional testing. The FDG-modules can be processed in single-step mode, and all external input signals can be inserted from the service unit. The results can be monitored by tracing internal and external signals.

- **DIAGNOSIS:**

In this mode, direct memory access is granted to the service unit. Special diagnosis programs can be downloaded from the service unit into RAM. Additionally, the target system debug functions are activated, so that debugging with an external debugger is possible.

To prevent unauthorized interference from the service unit, operation mode release signals control transitions between operation modes. These release signals are acquired either directly by input modules or via data messages. They are specified in function diagrams and passed to the RTE by a special interface function block.

The RTE also includes three sub-modules:

1. Input/output (I/O) drivers:

An I/O driver module is provided for every type of input/output module. The drivers transfer input/output signals between the RTE and the specific I/O module. The I/O drivers also initialize the I/O modules and detect I/O errors.

I/O modules are process interface modules between the different processors and the plant instrumentation. There are only nonprogrammable I/O modules in the TXS. All modules are on printed circuit boards with a connector to the backplane bus and a male multipoint connector for connecting test and monitoring equipment to the front panel. Analog modules contain an analog-to-digital converter and a multiplexer. The method of operation is always such that signal transmission between the signal buffers and the male multipoint connector toward the module operates independently of the data transmission between the module and the backplane bus. Accesses to the I/O modules by the function processors are by direct addressing via the backplane bus by module-specific software drivers that perform both data conversion and fault processing.

Monitoring equipment on I/O modules mainly aim at external circuitry. Failures in the interface with the backplane bus are detected and signaled by the function processors during their cyclic access to the signal buffers. The majority of failures concern signal input or signal output channels. If a multiplexer or a signal converter fails, the entire module is affected. Failures in the interface can, in rare cases, affect the backplane bus. Failures of the signaling equipment (e.g., light emitting diodes) do not have any effect on the safety functions.

2. Exception handler:

The exception handler module responds to unexpected situations, such as time-out, watchdog, or unexpected operating code exceptions. The exception handler saves information about the exception and its context for subsequent analysis of system behavior. Depending on the type of exception, the exception handler then either restarts the processing module (through a software-activated reset) or shuts down the processing module in a defined state. Information saved by the exception handler can be read from the service unit via services of the RTE or read directly via serial line connection from the front plate of the processing module.

3. Self-monitoring software:

The self-monitoring software performs a sequence of self-monitoring checks on the various hardware components of the processing module, such as RAM-test, FEPRM-test, and watchdog test. The self-monitoring is performed during time intervals when no cyclic processing of the FDG-modules is active. It is repeated

continuously, and its cyclic processing is monitored by the RTE. Any errors found are reported to the exception handler, which stores the information and takes care of the error handling.

The RTE has two major interfaces: the interface to the FDG-modules, and the interface to operating system software layer/target system hardware (target system interface). The FDG module interface consists of a set of unified functions. The RTE calls these interface functions via function pointers. The function pointers and the associated data structures and data types are defined in the RTE configuration module, which is generated by an automatic code generator (SPACE). These functions are described below:

- **Input function**

This function is used to pass input signals (from messages and/or input modules) to the function diagram (FD) modules contained in the FDG module.
- **Compute function**

This function is used to execute the computation of the FDG-modules. The compute function calls the associated FD compute functions in the correct order. These internally call the basic function blocks of each FD in the required order.
- **Output function**

This function is used to pass the calculated output signals of the FDG modules to the RTE. The signals are then sent via messages to output modules.
- **Interface function**

This function is an universal interface for read and write access to all FDG-module internal data structures, such as parameters, state variables, signals, etc. The RTE uses this interface function for accessing signals when tracing or changing the parameters of FDG-modules is required.

The target-system interface is the other major interface of the RTE. As a result of the nature of the system requirements, this interface is not as unified as the FDG-module interface. Basically, the target system interface consists of the following:

- **Operating system interface**

The operating system interface is restricted to an absolute minimum set of services: real-time related service (pause, task end, and resume after specified time interval), semaphore services, and event-flag services.
- **Communication software interface**

The communication software interface provides a unified interface for sending and receiving messages via communication channels. This is independent of the media used (media supported by the communication software are 32-Bit parallel backplane bus,

16-Bit parallel local extension bus, Ethernet 802.2/3 LAN, and Profibus LAN). Communication services are: create communication channels, send data via communication channels, receive data via communication channels, and get communication channel status.

- Target system hardware interface

The RTE also has a direct interface to certain components of the target-system hardware, either by direct access or by functions provided by HOT. This includes: access to LEDs on the processing module front-plate, EEPROM programming services, and watchdog services. The RTE target system interface, although not as unified as the FDG-module interface, has been designed to facilitate portability. This was accomplished by concentrating all target system-dependent interface functions in one sub-module, SYSTEM. Porting the RTE to another platform is done by adapting the module SYSTEM to the new platform.

On top of the RTEs internal module structure there are three modules, which control the three major functions of the RTE:

- Module INIT

This module is the central control instance during start-up of the RTE. It controls the complete initialization phase of the RTE. After the operating system has started the automatic startup tasks, the RTE monitoring tasks perform the RTE initialization and then start the RTE cycle task which starts operation in mode INIT. In this mode, the status of the input signal messages are checked. If all input signal messages are received satisfactorily (or when a timeout of typically 2 minutes has expired), the FDG-modules are initialized. After FDG initialization has been successfully completed, control is branched to the modules CYC and MONIT. If the initialization fails, cyclic operation will not be achieved and module INIT ends in an endless loop.

- Module CYC

This module is the top-most control module for the cyclic operation of the RTE. CYC uses services of underlying modules like FDGIFC (for interface to the FDG-modules), MODE (for handling operation mode transitions), or ERRORMSG (central error-message handling module).

- Module MONIT

This module controls the RTE interface to an external service unit. MONIT accepts a set of basic control commands, e.g., reading an error-message-buffer, requesting a change of operating mode, or setting a new parameter value. Not all control commands are permitted in every operating mode. For example, during normal operating mode OPERATION, only a very small subset of control commands is accepted by the RTE. This prevents unintended interference from the external service unit during normal operation.

The RTE, acting as a virtual machine, hides all target specifics such as hardware, operating system, communication media and protocols, and I/O modules from the FDG-modules. The RTE is activated cyclically by the operating system and then processes the following functions cyclically:

- resets the watchdog timer,
- increments the cycle counter,
- reads in the process data from the input/output (I/O) modules,
- reads messages from the dual-port RAM,
- transfers the data to the function diagram group modules,
- processes the function diagram group modules,
- checks fault messages from processing the function diagram group modules and sets the fault status signals,
- outputs the results of the function diagram group modules via the I/O modules,
- transmits messages to other function processors,
- activates service tasks if permissible manual control requests have been identified, and
- deactivates its own task until the next cycle.

At the beginning of the processing cycle, the RTE resets the watchdog timer to a value that is greater than the activation cycle for the RTE cycle time set in the operating system. If the RTE does not terminate correctly because of a fault in the signal flow, the watchdog timer times out and generates a hardware interrupt request. This interrupt request then activates a special interrupt service (the exception handler) that saves the current state of the processor for subsequent analysis and then puts the computer into a defined fault state. In this fault state, all output signals are set to predetermined states and the processor is kept in a waiting loop. The signal outputs are disabled in several different ways by explicit driver calls and by a hardware signal (BASP), which disconnects the local power supply for the I/O modules.

When the watchdog times out the first time, the hardware interrupt leads to an automatic reset (re-boot) of the CPU (it is assumed that a transient failure was responsible for the watchdog activation). During the automatic re-boot of the CPU the complete startup self-test is executed (in-depth check of the CPU hardware). In case the CPU passes the startup self-test it resumes the cyclic operation. If the watchdog times out again, the interrupt activated by the exception handler leads to the shutdown of the CPU (a severe hardware failure is assumed). A shut-down CPU can be re-activated only by re-setting the complete I&C subrack, which has to be done manually. However, prior to re-start of the CPU a complete check of the failure information would be appropriate.

The RTE also increments the local cycle counter. This 16-bit counter forms the internal relative short-time base sign-of-life clock for communication and for time-sequencing fault signals. The cycle count of the RTE at the time of transmission is appended to every message. This information is used by the receiving processor to monitor the validity of the message and the correct functioning of the transmitter.

Data are input and output via the I/O modules directly through driver programs that access the buffers of the I/O modules that are reading or writing the data. A separate driver program exists for each I/O module, and is also responsible for module-specific conversion of the data. Fault alarms that are detected on the I/O module (wire break, overflow, underflow) are used to mark the signals with the status "ERROR." Each configured signal in the TXS contains the

signal value and a signal status attribute with the status flags "Fault" and "Test." These flags are used for fault masking. Missing front connectors or a missing load power supply can result in the enable signal for addressing I/O modules not being formed. The missing enable signal is detected and signaled by the time-out monitoring. At the same time, the status flags are set to "ERROR" for all signals concerned so that these signals are not used in further signal processing.

The number of signal ERRORS and/or failures in the entire system that would be permitted before leading to the degradation of the safety function depends on the system architecture selected for the task to be fulfilled (such as for the reactor trip system and engineered safety feature actuation system). How long such a degraded system operation would be allowed is governed by the technical specification for a specific system application.

The function processor reads messages by direct accessing the local dual-port RAM. In safety-related applications, all messages contain additional data for monitoring system integrity at the application layer. This includes the cycle count of the RTE that transmitted the message, the message identification number, the message length, and a checksum with which the integrity of the data from the RAM of the transmitting function processor to the RAM of the receiving function processor is monitored. If the RTE detects that the cycle count has not been incremented properly in a received message, the receiving processor considers the data faulted and an up-circuit processor is no longer functioning properly. An incorrect checksum also indicates that the messages are inconsistent and must be excluded from all further processing. If the data received are current and consistent, they are passed on to the application functions (function diagram group modules).

For the master/checker pair of voter computers, the necessary signal exchange and result comparison between the redundant computers is performed by the runtime environment.

After transferring the data to the function diagram group modules, the RTE begins processing the data in the function diagram group modules. During normal system operations, this processing activity is assigned the highest priority, such that, if an operator requests a service function, the service function is not processed until after the function diagram group modules are processed. During function diagram group module processing, the RTE checks fault messages arising from the processing, and sets fault status signals for use by the exception handler. Details regarding the function diagram group modules are provided in the next section.

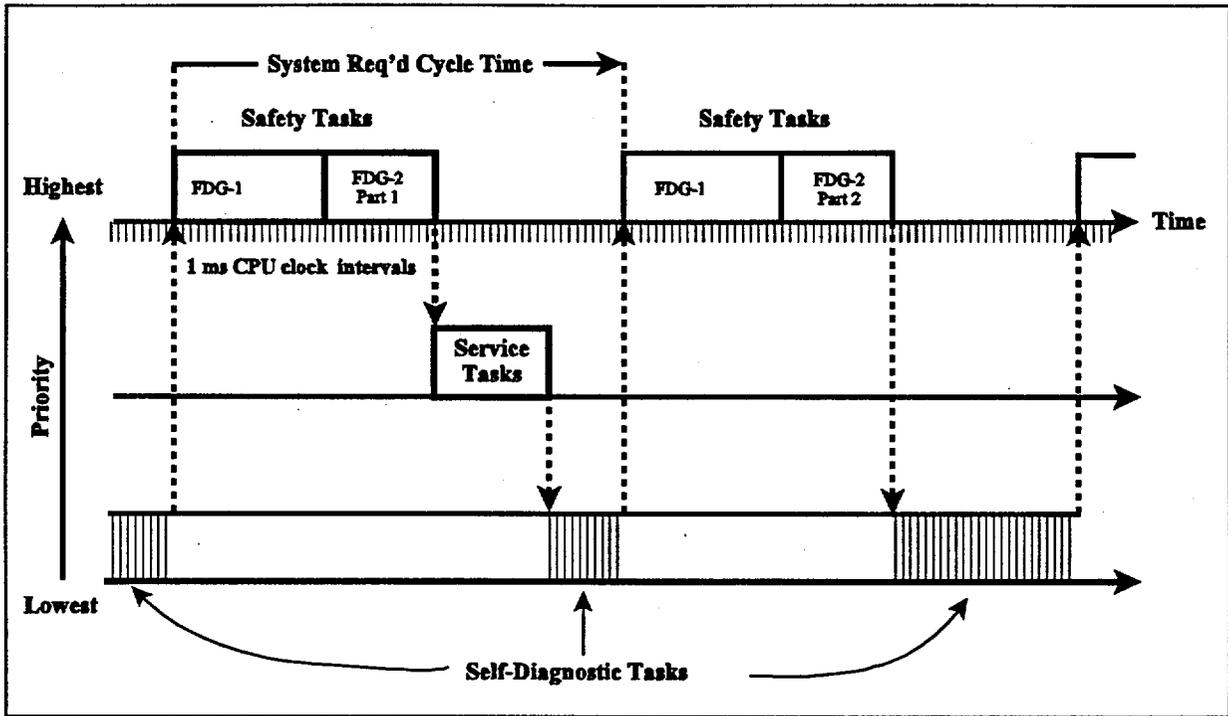


Figure 2. Task scheduling during normal operations.

Upon completing the processing of the function diagram group modules, the RTE places the processing results into the sending port of the dual-port RAM, for processing by the I/O modules. The I/O modules then process the results for subsequent transmission to other function processors.

If service tasks have been requested by the operator, these tasks are then scheduled for processing in the time remaining during the cycle (see Figure 2). The service tasks are kept from being processed by use of a semaphore, which is held by the safety function. After the safety function is processed, the semaphore is passed to the service task for one clock cycle (1 ms). The service task retains the semaphore for that clock cycle then returns the semaphore to the RTE. If the cycle time has not elapsed, the RTE passes the semaphore back to the service task for further processing. This exchange of a semaphore continues until the service task is completed or the cycle time expires, whichever occurs first. Using this technique, the safety function retains the highest priority for system resources.

Upon completion of the safety function(s) and the service task(s), the RTE deactivates its own task until it is again activated by the operating system scheduler at the start of the next operating cycle. During this time period, the operating system activates the self-test functions, which are processed in 1-ms time increments until the next scheduled processing cycle is to begin. The operating system scheduler then activates the RTE for processing the safety functions. The 1-ms time increments are used to ensure that safety function processing is performed at the required frequency.

RTE provides computing time monitoring. If the computing time is greater than the cycle time minus 2ms, an error message is generated. The RTE also monitors execution of the cyclic

self-monitoring. If not completed after a specified time, an error message is issued and sent to the service unit, and to the exception handler which will immediately shutdown the CPU. In addition, RTEs in the various system CPUs receive messages from each other and monitor the message age. By this means the sender's cyclic operation is monitored independently by other RTEs. Furthermore, the watchdog timer monitors execution of the RTE's cyclic task, and is activated after a very short period of time following the start of the last cycle if a problem is detected.

The TXS system automatically detects failures in the subracks, the function processors, the I/O modules, and the communication functions. Failures that affect the subrack internal power supplies or control of the backplane bus will cause a transition to predefined fault conditions (e.g., reset) on the function computers, which results in a nonresponsive state in relationship to other subracks. Additionally, the TXS system monitors cabinet temperatures and cabinet cooling fan speed and provides the plant operators with an alarm if setpoints are exceeded.

The function processors are designed so that two independent monitoring systems for detecting failures could affect safety system operation. One approach for detecting failures is the strictly cyclical use of all hardware components. The watchdog timer and the system support controller provide this monitoring capability. The watchdog timer monitors program operation and the system support controller monitors hardware access times. The hardware times monitored by the TXS system are:

- access times and time-out times on accesses to the I/O bus and the backplane bus, and
- the waiting time for allocation of the backplane bus.

The cyclic self-monitoring function also addresses:

- the integrity of the data permanently stored in the flash EPROM and in the EEPROM by use of CRC checks,
- the function of the read and write memory,
- the function of the processor and coprocessor,
- the function of the timers, interrupts, and watchdogs,
- the function of the I/O ports, and
- the correct setting of the jumpers.

These monitoring capabilities ensure the detection of function processor failures that could affect safety system operations.

Monitoring functions for the I/O modules primarily address wire breaks, connectors, and measuring ranges. Consequently, a failure of the module itself is only partly detected by system-inherent equipment. Failures in the interface with the backplane bus are detected and signaled by the cyclic accesses of the function processors to the signal buffers. The majority of failures concern signal input or output channels. If a multiplexer or a converter component fails, the entire module is affected. In unusual cases, a failure in the interface can also affect the backplane. Failures of LEDs (light emitting diodes) and other signaling equipment do not affect the safety function of the system. The use of voting, which uses redundant signals to arrive at a safety state, provides assurance that a single failure in an I/O module will not affect the safety function.

TXS communication functions have three independent methods of detecting failures. These methods are the LAN protocol detection mechanisms, the communication processor detection processes, and the CRC on the application layer. Using these three methods, the TXS can detect component failures that are restricted to the bus interface, component failures of an entire module, and component failures that affect an entire subrack or an entire bus segment.

Typically, communication failures affect the links that serve failed equipment. For equipment connected to the subrack, failures of the interface with the backplane bus can affect the entire subrack. Modules that function directly on the serial bus can cause an entire bus to fail. These types of failures are easily detected by the system.

Configured monitoring mechanisms in the TXS make use of redundant information processing with subsequent voting of the results. By comparing information from redundant channels, the TXS can detect deviations in the redundant signals and so identify module failures. Four basic types of configured monitoring mechanisms are used in the TXS system: redundant measured value processing, configured monitoring of I/O modules, use of master-checkers for comparing results, and use of voters.

In nuclear power plant safety systems, safety-related values are acquired and processed in redundant channels. One way TXS systems process redundant signals is to use the signals to determine a real time best-estimate representation of the actual process being measured. The process for obtaining this best-estimate value is usually by voting the appropriate signals and then selecting the best-estimate value from the result of this voting. For example, the voting process could use the second highest value of four signals for selecting the signal to be used for actuating a safety system on a high trip setpoint. This process also allows the system to monitor the consistency of the signals. All failures that do not result in a "frozen" value can be detected with redundant measured value processing.

The TXS system applies test signals to each TXS safety circuit to continuously monitor the I/O modules. The test signals are monitored to ensure the I/O modules are correctly processing the signals. The degree of monitoring depends on the safety function to be performed. This method of detecting I/O module failures is only incrementally better than redundant value processing at detecting failures.

For output modules that control important items of safety equipment, another method is to read back and compare output signals for consistency with the expected value. The advantage of this method is that, for frequently used equipment, equipment errors may be detected before the failure has a significant effect on safety.

2.2.1.3 Application Software

The application software performs the plant-specific TXS safety-related functions using function block modules, function diagram modules, and function diagram group modules.

Function block modules perform all numeric operations involving input signals. These operations include basic functions such as adding signals, integrating signals, and comparing signals to predefined values. These function blocks are available in the form of type-tested libraries. Each function block module is associated with a data structure that contains the input data, output data, all buffer addresses, and parameters specific to the function of that module.

These data structures allow complete verification of each calculation step in the processing sequence. Within a processing cycle, all temporary data are preserved and not overwritten. At the end of the cycle, these data can be transmitted to the service unit for subsequent system maintenance, diagnostic activities, and status tracking.

All function block modules process the value and status of their input signals. The signal status is an attribute that indicates the quality of the output signal. Function block modules have either active-status processing or passive-status processing. For passive-status processing, the output signal of a function block is simply formed by OR gating the status information of all signals. Using passive-status processing, any signal marked as faulted causes the resulting signal of the function block to contain the attribute ERROR. For function blocks with active-status processing, the resulting signal is only calculated from fault-free input signals so that the output signal is also marked as fault-free. In this case, a fault-free output signal can only result if the input signals give mutually redundant information. Active-status processing, therefore, is only possible with function blocks that perform selection and majority voting functions. These include blocks such as for second-maximum, second-minimum, and "m-out-of-n" coincidence logic. Function blocks with active-status processing are used to screen, or mask, faulted signals and thereby prevent their propagation to the next function. Function blocks are not plant-specific functions. Rather, these blocks are stored in a development system library for use by system designers.

Function diagram modules consist of groupings of function blocks that are used for plant-specific applications. The function diagram modules are developed from plant-specific function diagrams using an automated and qualified generation process. The function diagrams are composed of graphic function blocks that represent a separately testable function. Once the function diagram is completed, the diagram is converted into a database, from which the graphical application is developed into function diagram modules, which have corresponding predefined software modules. The function diagram modules are activated by the runtime environment in the form of function calls. All safety functions are specified as function diagrams.

Function blocks are connected by signals via their input and output ports. Each port has an associated type, which defines the type of signal that can be connected to it. Three types of signals are defined in the TXS: analog (float valued) signals, binary (boolean valued) signals, and message signals.

The rules that define the connectivity of function blocks are based on the signal types of the ports. Only ports of the same type can be connected by a signal. This is checked on-line during the specification of a function diagram by the graphical TXS editor.

An underlying restriction is imposed for message signals. Each message signal is of the generic type, although the bit-mapped message code is specific to each function block type. As a result, for example, the message signal output port of the function block that evaluates two or more trip signals out of four signals may not be connected to the message signal input port of a different type of message decoder even though both ports are of the same generic type. This type checking is performed at runtime by the message decoders themselves, based on the function block (FB) information that is part of each message signal.

Because several function block modules are typically implemented in one processor, all function diagram modules that are to be processed with the same cycle time are grouped together to form function diagram group modules. A function diagram group module therefore consists of a sequence of calls to function diagram modules and copy functions by which signal transfers between the function diagram modules are implemented. A function diagram module consists of a sequence of calls to function block modules that are interconnected by data structures. Function diagram group modules are stored in the flash EPROM on the system processor printed circuit board.

Two function diagram group modules can be implemented on one function processor. The processing cycle time of the runtime environment corresponds to the cycle time of the faster function diagram group module. Processing of the slower function diagram group module is distributed over several basic cycles to achieve a constant load distribution. The allocation of the function diagram group processing to several basic cycles is generated explicitly by the code generator. Function diagram modules and function diagram group modules do not use system services. Only the runtime environment is responsible for supplying data and passing on the results by calling the required copy functions and initiating output communication requests.

Function blocks in different function diagrams (FD) are connected in the same way as they are within the same FD. The only difference is that the connecting signals must be exported by the source FD and imported by the receiving FD. Each signal gets a unique name code, based on the name code of the source FD. This is in contrast to local signals within a FD, which are not identified by a unique FD name code.

The TXS conceptual architecture supports the software specification, the hardware specification, and the software-hardware interface. The software specification consists of the function diagrams discussed above. The software specification is independent of the target system and is a formal, domain-specific specification that defines the signal processing used to implement the elementary safety functions defined by the system requirements specification. The software specification is created using the TXS editor.

The hardware specification contains the complete hardware structure of the target system, with all its hardware components. For this specification, hardware diagrams and hardware blocks representing the target system hardware components are used. The hardware specification is also created using the TXS editor.

After creating the hardware and software specifications, each function diagram is assigned to one processing module. This assignment is done while creating the hardware diagrams, by adding the function diagram identification to the parameter list of the processing module using the TXS Editor. The information for the integrated system design is stored in the specification database.

The complete specification captures functional aspects and the system's detailed hardware structure. Nonfunctional aspects such as independence constraints, fault tolerance, and timing requirements are also implicitly contained in the specification. The specification can be prepared by I&C engineers using notations and methodologies that have been common practice in the I&C community. The software specification remains independent of the specific details of the target system. The verification of the specification by the process engineers who

prepared the system requirement specification is facilitated by the use of a commonly understood notation.

The specification is formal in the sense that all information needed to implement the final code running in the distributed target system is available from the specification database. Also, certain verification procedures such as check of completeness, unambiguity, consistency with naming scheme, and parameter checks can be done automatically at specification time. Using the formal specification and a set of predefined rules, the target system code is generated automatically, thus improving code quality and reducing costs. On the other hand, by applying the inverse rules, the generated target system code is analyzed by independent tools and compared to the original database representation.

2.2.2 Software Documentation

This section summarizes the software documentation associated with the TXS system development. The type tests of the TXS software components were performed in accordance with German standard KTA-Standard 3503. The principles of type testing and the test activities were defined from this standard. These were applied to the following areas: separation in the theoretical and practical tests, institutions to be involved in type tests, roles of these institutions in type tests, and documentation of type tests.

The content of the theoretical and practical tests is defined by the software standard DIN IEC-880.

KTA standards also require that the present state-of-the-art be taken into account during the qualification. In addition to KTA-1401, which defines criteria for quality assurance systems, the following software standards were applied and verified:

- ISO-9000-3, "Management for Quality and Requirements of Quality Assurance,"
- IEEE-830, "Software Requirement Specifications,"
- IEEE-828, "Software Configuration Management Plan,"
- IEEE-1012, "Software Verification and Validation Plans,"
- IEEE-829, "Software Test Documentation,"
- IEEE-1008, "Software Unit Testing,"
- IEEE-1028, "Software Reviews and Audits," and
- ANSI/ANS-10.4, "Verification and Validation of Scientific/ Engineering Programs for the Nuclear Industry."

Among the standards referenced in the Standard Review Plan and the Branch Technical Positions, IEEE-7-4.3.2 gives specific requirements concerning software development. Most of these requirements are given by reference to the standards ASME NQA-10.4, IEEE-730, IEEE-828, IEEE-1012, and IEC-880. The requirements of ASME NQA-10.4 are covered by KTA -401, and the requirements of IEEE-730 are covered by ISO-9000-3. All other standards were directly applied in the development and evaluated in the type tests.

2.2.2.1 Vendor/Customer System Specification

Documentation supporting the system specification will be reviewed on a plant-specific basis.

2.2.2.2 Software Management Plan

The software management plan for development of a Siemens digital safety system is the same procedure as used for all Siemens safety-critical software development projects. The software management plan is incorporated into Siemens Engineering Procedure FAW-1.1, "Software Life-Cycle Processes." FAW-1.1 specifies the management structure and the processes to be used in the project. This procedure is compatible to IEEE-1074, "Developing Life Cycle Process," and is, therefore, acceptable.

2.2.2.3 Software Development Plan

The software development plan is documented in Siemens Engineering Procedure FAW-1.1, "Software Life-Cycle Processes." This procedure defines the software life cycle processes to be used in the development of a safety-related digital system.

2.2.2.4 Software Quality Assurance Plan

The software quality assurance plans are incorporated into three Siemens Engineering Procedures, FAW-3.4, "Contents and Structure of System Specifications for Software Components," FAW-3.5, "Contents and Structure of Design Documents for Software Components," and FAW-3.6, "Contents and Structure of Implementation Documents for Software Components." FAW-3.5 describes the process by which the software specification is translated into the software design description. FAW-3.6 describes the process by which the software design description is implemented. The staff has reviewed these procedures and found that these procedures are compatible to the U.S. IEEE standards listed in the NRC SRP Chapter 7, therefore, the staff considered these procedures acceptable. Additional Siemens corporate quality assurance procedures include EMF-1, Part II, Rev. 29, "Siemens Power Corporation Quality Assurance Manual for Nuclear Fuels and Services" (approved by the NRC by letter dated June 11, 1998), and QMH 12E KWU NL, "Quality Program, Quality Manual Handbook for Nuclear Services."

2.2.2.5 Software Configuration Management Plan

Configuration management activities are controlled by Siemens Engineering Procedure FAW-1.5, "Configuration Management," which outlines the procedures and tools for creating and implementing the configuration management structure and procedures. This procedure is compatible to IEEE-828, "Software Configuration Management Plan," and is, therefore, acceptable.

2.2.2.6 Hardware and Software Specification

The procedure for controlling the hardware and software specifications is Siemens Engineering Procedure FAW-3.3, "Organization of the General Specification for SW and HW Components." This procedure governs the organization of the specifications for the digital safety systems created under this set of tools and processes. This procedure is compatible to IEEE-830, "Software Requirement Specifications," and is, therefore, acceptable.

2.2.2.7 Software Requirements Specification (SRS)

The software requirements specifications are controlled by Siemens Engineering Procedure FAW-3.4, "Contents and Structure of System Specifications for Software Components," and FAW-3.5, "Contents and Structure of Design Documents for Software Components." FAW-3.4 describes the process to be used for converting the system requirements into software specifications. FAW-3.5 describes the technical processes for converting the software specification into a module structure that may be used for implementing the software requirements. These procedures are compatible to IEEE-7-4.3.2, "IEEE Standard for Digital Computers in Safety Systems of Nuclear Power Generating Stations," and are, therefore, acceptable.

2.2.2.8 Software Requirements Review (SRR)

The processes by which software requirements are reviewed are described in Siemens Engineering Procedure FAW-4.2, "Reviews." This procedure describes the software review process, including responsibilities, review methods, the review processes, and activities to be performed after the review is completed. This procedure is compatible to IEEE-1028, "Software Review and Audit," and is, therefore, acceptable.

2.2.2.9 Software Design Description (SDD)

The processes controlling the software design description are specified in Siemens Engineering Procedure FAW-3.5, "Contents and Structure of Design Documents for Software Components," and FAW-3.6, "Contents and Structure of Implementation Documents for Software Components." FAW-3.5 describes the process by which the software specification is translated into the software design description. FAW-3.6 describes the process by which the software design description is implemented. These procedures are compatible to IEEE-7-4.3.2, "IEEE Standard for Digital Computer in Safety Systems of Nuclear Power Generating Stations," and are, therefore, acceptable.

2.2.2.10 Software Design Review (SDR)

The processes by which software design is reviewed are described in Siemens Engineering Procedure FAW-4.2, "Reviews." This procedure describes the software review process, including responsibilities, review methods, the review processes, and activities to be performed after the review is completed. This procedure is compatible to IEEE-1028, "Software Review and Audit," and is, therefore, acceptable.

2.2.2.11 Source Code Listing

The structure of the source code listings is specified in Siemens Engineering Procedure FAW-2.1, "Coding Rules." These rules are incorporated into the SPACE tool, which generates the function diagram modules and function diagram group modules. FAW-2.1 provides specific programming guidelines for the C, C++, and FORTRAN 77 software languages. Source code listings of specific applications will be reviewed on a plant-specific basis. This procedure is compatible to IEEE-1028, "Software Review and Audit," and is, therefore, acceptable.

2.2.2.12 Source Code Review

The processes by which software requirements are reviewed are described in Siemens Engineering Procedure FAW-4.2, "Reviews." This procedure describes the software review process, including responsibilities, review methods, the review processes, and activities to be performed after the review is completed. This procedure is compatible to IEEE-1028, "Software Review and Audit," and is, therefore, acceptable.

2.2.2.13 Safety Analyses

Safety analyses of specific applications are the licensee's responsibility and will be reviewed on a plant-specific basis.

2.2.2.14 Software Verification and Validation Plan (SVVP)

The processes for conducting software verification and validation (V&V) activities are described in Siemens Engineering Procedure FAW-1.6, "Verification and Validation Plan." FAW-1.6 specifies the areas of application, the organizational responsibilities, requirements for IV&V activities, and requirements for documentation. This procedure is compatible to IEEE-1012, "Software Verification and Validation Plans," and is, therefore, acceptable. The requirements for V&V are described in IEC-880-1986, "Software for safety Systems in Nuclear Power Stations," which Siemens has followed throughout the life cycle. IEC-880 is compatible to IEEE-7-4.3.2, "IEEE Standard for Digital Computers in Safety Systems of Nuclear Power Generating Stations," and is, therefore, acceptable. Additionally, an IV&V plan has been prepared by the IV&V groups TÜV Nord and iSTec, which are working under a subcontract for the German Reactor Safety Association, which has a contract with the Bavarian nuclear licensing authority to perform third party software type tests.

2.2.2.15 Verification and Validation (V&V) Report

Verification and validation reports are prepared by Siemens for each specific application and for each component of the application development database. The staff reviewed V&V reports for three components during its audit of Siemens in December 1999 and found the reports acceptable as discussed in Section 4.4 below.

2.2.3 Development and V&V Organization and Process

The V&V processes are defined in Siemens Engineering Procedure FAW-1.6, "Verification and Validation Plan." This plan specifies all activities performed during the safety system development process. The responsibility for V&V activities is with the person responsible for the system or module development. This procedure is compatible to IEEE-1012, "Software Verification and Validation Plans," and is, therefore, acceptable.

Siemens internal V&V processes were performed by members of the same development team, a member of another team within the digital I&C organization, or by employees outside the digital I&C organization. The person performing the internal V&V activity was not the same person who generated the product to be reviewed. External IV&V activities were performed by TÜV organizations and iSTec.

The person responsible for ensuring the V&V activities are performed develops the draft development document. This person then assigns the document draft status and releases the document for a consistency check and a technical review. The consistency check of the draft document is normally performed by a member of the V&V team. The purpose of the consistency check is to ensure that all interfaces to adjacent components have been considered.

The participants of the technical review follow the requirements of FAW-4.2, "Reviews." The participants for this review are equivalently qualified and are not involved in the generation of the document to be reviewed. The results of the review are incorporated into the draft document by the person responsible for the document. The resulting document is made available for external verification and review.

Next comes external verification of the development documents for components that do not involve a specific plant application, which involves verifying that the safety-related features of the system have been correctly incorporated into the safety system. A final check of the verified documents is then performed, and the resulting documents are sent to the testing organization for checking the external modification requirements.

The project manager has the final approval responsibility of the documents.

Validation activities include testing the application to ensure it performs according to the system requirements. These activities are controlled by Siemens Engineering Procedure FAW-4.1, "Testing." Testing includes specifying the test requirements, performing the tests, and producing the test report. Testing includes module testing, component testing, and system testing in a simulated and real environment. This procedure is compatible to IEEE-1008, "Software Unit Testing," and is, therefore, acceptable.

Documentation of the test results includes verification of the phase results, validation of the test specification, and integration of the component into the system.

Siemens performed V&V activities during each phase of the software development. The purpose of the activities was to verify that the requirements were correctly addressed throughout the software life cycle (component specification, component design, implementation, and testing). The system integration and operations phases are plant specific, and the associated V&V activities and documentation will be reviewed on a plant-by-plant basis.

2.2.4 Configuration Management

Configuration management activities are controlled by Siemens Engineering Procedure FAW-1.5, "Configuration Management." This procedure provides the requirements and 71 procedures necessary for maintaining configuration control of the project. The procedure defines the configuration requirements and specifies the processes for generating configuration identifiers, controlling changes, and maintaining version control during the development process. Configuration identification is applied to all software and associated documentation.

Baselines are established to control design, product, and engineering changes. These baselines are defined by the configuration manager, and cannot be changed without approval

of the configuration control board. The procedure to change a configuration item consists of the following steps:

- A change request is prepared by the person requesting the change.
- The development group evaluates the change.
- A proposal describing the process for making the change is prepared.
- The development group recommends disposition of the change request.
- The configuration item is changed according to the approved change request and proposal for change.

Software configuration management and control is applied to all documents and software code. This control is implemented using the configuration identification number assigned by the configuration manager.

Siemens maintained the documentation of configuration management for the TXS system platform that includes long-term service with compatible hardware and software components. Siemens also maintained the documentation of project-specific configuration management activities that include project-specific application software consistent with functional requirements. Every hardware and software component has a certification that identifies the modification version of that component.

The staff found that the configuration management procedure FAW-1.5 is compatible to IEEE-1042, "IEEE Guide to Software Configuration Management," and is, therefore, acceptable. However, the licensee should demonstrate that the plant-specific configuration management activities have been carried out in the life cycle process implementation. Documentation should exist that shows the configuration baselines have been established for the activity group, and an adequate change control process has been used for changes to the product baseline. This is a plant-specific action item.

3.0 REVIEW CRITERIA AND METHOD OF REVIEW

3.1 Review Criteria

The following acceptance criteria and guidelines for reviewing a safety-related reactor protection system such as the TXS system are identified in the Standard Review Plan (NUREG-0800), Sections 7.1 and 7.2:

1. 10 CFR Part 50, §50.55a(h), "Protection and Safety System."
2. General Design Criteria 2, "Design Basis for Protection Against Natural Phenomena."
3. General Design Criterion 4, "Environmental and Missile Design Basis."
4. General Design Criterion 20, "Protection Systems Functions."
5. General Design Criterion 21, "Protection System Reliability and Testability."
6. General Design Criterion 22, "Protective System Independence."

7. General Design Criterion 23, "Protection System Failure Modes."
8. General Design Criterion 24, "Separation of Protection and Control Systems."

The following regulatory guides and industry standards provide information, recommendations and guidance and, in general, provide an acceptable basis to implement the above requirements for both hardware and software features for safety-related digital systems such as the TXS system:

1. Regulatory Guide 1.152, "Criteria for Programmable Digital Computer System Software in Safety Related Systems of Nuclear Power Plants."
2. IEEE Standard 7-4.3.2-1982, "Application Criteria for Programmable Digital Computer Systems in Safety Systems of Nuclear Power Generating Stations."
3. IEEE Standard 323-1974/1983, "IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations."
4. IEEE Standard 338-1987, "IEEE Standard Criteria for Periodic Testing of Nuclear Power Generating Station Safety Systems."
5. IEEE Standard 344-1987, "IEEE Recommended Practices for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations."
6. IEEE Standard 379-1988, "Application of the Single Failure Criterion to Nuclear Power Generating Station Class 1E Systems."
7. IEEE Standard 384-1992, "Criteria for Independence of Class 1E Equipment and Circuits."
8. IEEE Standard 472-1974, "Guide for Surge Withstand Capability Tests."
9. IEEE Standard 730-1989, "Software Quality Assurance Plans."
10. IEEE Standard 828-1990, "Software Configuration Management Plans."
11. IEEE Standard 829-1983, "Software Test Documentation."
12. IEEE Standard 830-1984, "Guide for Software Requirements Specifications."
13. IEEE Standard 1012-1986, "IEEE Standard for Software Verification and Validation Plans."
14. IEEE Standard 1016-1987, "IEEE Standard for Recommended Practices for Software Design Descriptions."
15. IEEE Standard 1028-1988, "IEEE Standard for Software Reviews and Audits."

16. MIL-Std-461, "Electro-magnetic Emission and Susceptibility Requirements for the Control of Electro-magnetic Interference."
17. MIL-Std-1399, "Interface Standard for Shipboard Systems, DC Magnetic Field Environment."
18. IEC-801-2, "Electromagnetic Compatibility for Industrial-Process Measurement and Control Equipment Part 2: Electrostatic Discharge Requirements."
19. SAMA PMC 33.1-1978, "Electro-magnetic Susceptibility of Process Control Instrumentations."
20. ASME NQA-2a-1990, Part 2.7, "Quality Assurance Requirements of Computer Systems for Nuclear Facility Applications, American Society of Mechanical Engineers."
21. EPRI Topical Report TR-107330, "Generic Requirements Specification for Qualifying a Commercially Available PLC for Safety-Related Applications in Nuclear Power Plants." TR-107330 was approved by NRC on July 30, 1998.
22. EPRI Topical Report TR-102323-R1, "Guidelines for Electromagnetic Interference Testing in Power Plants." TR-102323-R1 was approved by NRC on April 30, 1996.

3.2 Method of Review

The purpose of the NRC review is to determine whether the proposed use of equipment and other technical requirements provide reasonable assurance that the applicant or licensee will comply with the Code of Federal Regulations, Title 10, Chapter I, and that the public health and safety will be protected. The review, audit, or inspection activities are not intended to completely evaluate all aspects of the design and implementation of the Siemens TXS I&C system. The review scope was sufficient to allow the reviewer to reach the conclusion of reasonable assurance described above.

This topical report was submitted for generic review, and will be referenced in the future for a plant protection system upgrade or replacement. To ensure that the digital plant protection system will perform its safety function as designed, the staff concentrated on the basic operation of the TXS software system, the life cycle activities of TXS hardware and software systems, and the qualification testing. Meetings were held at the NRC office on October 14 and 15, 1999, and November 16, 17, and 18, 1999, and an audit review meeting was held at Siemens' office on December 6 - 10, 1999.

Based on previous advanced reactor digital I&C systems reviews, the staff developed a generic digital safety evaluation outline. The outline describes the kinds of information the staff needs to address in the safety evaluation for a complex digital I&C upgrade system. This outline was provided to Siemens as a framework for the agenda of the meetings listed above. A documentation audit was conducted at Siemens office in Germany to verify the information related to the TXS system life cycle activities. The staff made a site visit to a German nuclear power plant GKN (Gemeinschaftskernkraftwer) to observe the TXS system in operation. The plant operators demonstrated the operation, diagnosis, and maintenance capabilities of the TXS system and discussed the experience of changing from an analog system to a digital

system. The plant operators stated that they are very pleased with the capabilities and maintainability of the new digital system.

The staff has also relied on nuclear industry efforts to establish an appropriate qualification program for upgrading I&C systems in nuclear power plants. The EPRI Topical Report TR-107330, "Generic Requirements Specification for Qualifying a Commercially Available PLC for Safety-Related Application in Nuclear Power Plants," describes the generic functional and the qualification requirements for a PLC (programmable logic controller) and provides guidance on implementing PLC-based applications. TR-107330 was endorsed by NRC (SE dated July 30, 1998). The staff will require a licensee referencing the TXS system for upgrading I&C systems to meet the seismic and environmental qualification requirements specified in TR-107330. Likewise, the licensee should meet the EMI/RFI qualification requirements specified in EPRI TR-102323-R1, "Guidelines for Electromagnetic Interference Testing in Power Plants," (NRC SE dated April 17, 1996).

4.0 SYSTEM EVALUATION

This section discusses the defense-in-depth and diversity assessment of the TXS system, surveillance testing, system response time testing, and software lifecycle evaluation of the TXS.

4.1 Defense-in-Depth and Diversity (D-in-D&D) Assessment of the TXS System

The staff described concerns with common-mode failures and other digital system design issues in SECY-91-292. SECY-91-292 describes how common-mode failures could defeat the redundancy achieved by the hardware architectural structure, and also result in the loss of several echelons of defense-in-depth (provided by the monitoring, control, reactor protection, and engineered safety functions performed by the digital I&C systems).

The staff has established acceptance guidelines for D-in-D&D assessments and has identified four echelons of defense against common-mode failures:

- Control system - The control system echelon consists of nonsafety equipment which routinely prevents reactor excursions toward unsafe regimes of operation, and is used for normal operation of the reactor.
- Reactor trip system (RTS) - The reactor trip echelon consists of safety equipment designed to reduce reactivity rapidly in response to an uncontrolled excursion.
- Engineered safety feature actuation system (ESFAS) - The ESFAS echelon consists of safety equipment which removes heat or otherwise assists in maintaining the integrity of the three physical barriers (cladding, vessel, and containment) to radioactive release.
- Monitoring and indication - The monitoring and indication echelon consists of sensors, displays, data communication systems, and manual controls required for operators to respond to reactor events.

As a result of the reviews of advanced light-water reactor (ALWR) design certification applications that used digital protection systems, the staff documented its position in SECY 93-087, "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and

Advanced Light-Water Reactor Design," with respect to common-mode failure in digital systems and defense-in-depth. This position is also documented in the SRP BTP HICB-19, "Guidance for Evaluation of Defense-in-Depth and Diversity in Digital Computer Based Instrumentation and Control Systems." Points 1, 2, and 3 of this position, described below, apply to digital system modifications for U.S. operating plants:

1. *The applicant/licensee should assess the diversity and defense-in-depth of the proposed instrumentation and control 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 those events.*
3. *If a postulated common-mode failure could disable a safety function, then a diverse means, with a documented basis that the diverse means is unlikely to be subject to the same common-mode failure, should be required to perform either the same function or a different function. 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.*

The two principle factors for defense against common-mode/common-cause failures are quality and diversity. Maintaining high quality increases the reliability of both individual components and complete systems. The TXS system quality has been described in Sections 2.1.3 and 2.2.1 of this safety evaluation. The staff requested Siemens to provide additional information to address the defense-in-depth and diversity in the TXS design. By letter NRC:99:037, dated September 1, 1999, Siemens submitted Technical Report EMF-2267(P), "Siemens Power Corporation Methodology Report for Diversity and Defense-in-Depth." The report addresses diversity and defense-in-depth for applications involving replacement of obsolete analog instrumentation in operating nuclear power plants.

The Siemens methodology follows acceptance criteria stated in SRP BTP HICB-19 and recommends that the applicant/licensee's diversity and defense-in-depth analysis follow the detailed guidance of NUREG/CR-6303, "Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems."

By letter NRC:00:004, dated January 13, 2000, Siemens submitted proprietary report EMF-2340(P), Revision 0, "Siemens Power Corporation Typical Diversity and Defense-in-Depth Assessment in Accordance with the Methodology of EMF-2267(P)." The purpose of this assessment is to demonstrate a typical PWR I&C upgrade with a TXS platform. The report defines a primary protection signal as the one which the protection function first occurs in the licensing basis analysis, and the backup protection signal (or signals) as those to occur if the primary protection function fail to actuate.

After evaluating each event, the report divides events into four categories:

- Category 1 Events that do not rely on functions processed by TXS for either primary or backup mitigation.
- Category 2 Events that do not rely on TXS for primary mitigation, but have a backup actuation processed by TXS.
- Category 3 Events that credit a TXS function for primary mitigation, but receive backup t6d backup mitigation. Operator action would be necessary to initiate manual actuations for these events. The indications and information available to allow the operator to initiate the appropriate actions are discussed in each event analysis.

The Siemens diversity and defense-in-depth methodology credits the inherent diversity between the TXS and TXP (control system) products. During a meeting at NRC on October 15, 1999, Siemens made a detailed presentation on the diversity between the TXS and TXP systems and the following are the major differences between the two systems:

- The design architecture are completely different.
- The design organization, management, designers, programmers, and testing engineers are different.
- The microprocessor CPU, input/output circuit boards and bus structure are from different manufacturers.
- The AC/DC power supplies and DC/DC power supplies are from different manufacturers.
- The computer 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.

On the basis of its review, the staff found that Siemens' diversity and defense-in-depth assessment methodology as described in EMF-2267(P) is consistent with the staff position stated in SRP BTP HICB-19 and is, therefore, acceptable. Applications following this methodology for a plant-specific diversity and defense-in-depth assessment should be found acceptable for this area. The actual review and verification of the major differences between the TXS and TXP was outside the scope of staff review. This is a plant-specific action item.

4.2 Surveillance Testing of the TXS System

By letter NRC:99:056, dated December 28, 1999, Siemens submitted report EMF-2341(P), "Generic Strategy for Periodic Surveillance Testing of TELEPERM XS Systems in U.S. Nuclear Generating Stations," for staff review. By letter NRC:00:017 dated March 3, 2000, Siemens provided additional clarification on recommended periodic surveillance test requirements for TXS applications. The report describes measures to be implemented in safety I&C systems configured with a TXS architecture to comply with requirements for channel checks, functional tests, channel calibration verification tests, response time verification tests, and logic system functional tests.

The measures include:

- Periodic verification (during refueling outages) of accuracy and time constants of the analog input modules.
- Continuous self-monitoring and on-line diagnostics to verify proper functioning of digital systems and to ensure integrity of the installed application and system software.
- Periodic actuation of output channel interposing relays. The reactor trip function is tested at the same surveillance test interval as current technical specifications (typically quarterly) and the engineered safety features actuation system (ESFAS) function is tested consistent with the licensee's refueling outage (typically 15 to 24 months).

As defined in the ALWR Standard Technical Specifications, a logic system functional test is a test of all required logic components (i.e., all required relays and contacts, trip functions, solid-state logic elements, etc.) of a logic path, from as close to the sensor as practicable up to, but not including, the actuated device, to verify operability. The logic system functional test may be performed by means of any series of sequential, overlapping, or total system steps so that the entire logic system is tested.

For some applications, interposing relays may be used in the logic component. The licensee should test those relays in accordance with the existing TS requirements. It is prudent to verify the logic system functions at least every refueling outage. This is a plant-specific action item along with the plant-specific technical specification requirements.

4.3 System Response Time Test

The TXS system response time testing is performed in overlapping steps:

- Verification of time constants of the input channels during input module tests, and
- Verification of the signal propagation time within the digital system

The accuracy and response time of the analog input channels are tested periodically by injection of test signals in the input circuits. An external test computer will be temporarily connected to the I&C system via permanently installed test plugs. While the input from the process is deactivated, calibrated electrical signals are generated and acquired. The digitized values are transmitted within the TXS system to the service unit and fed back to the test computer via a local network connection within the cabinet.

To verify the signal propagation time, two system properties of the TXS permit testing of the response time during operation without affecting the safety function:

- All signals are transferred from one computing node to the next strictly cyclically (it will never stop or wait for incoming data). Thus, even if the response time varies, it is the same for all signals using the same communication path.
- Actuation of one application function does not affect other application functions running on the same hardware resources.

As a means for verifying the reaction time of the logic, a binary input is provided to the data acquisition computers. Signal distribution to other computers is designed in the application software (functional diagrams) in the same way as for the normal measuring signals. Separate outputs are provided in the voting computers for each path. During periodic tests, the test machine connected to the I&C system generates a start signal and measures the reaction time of each signal path separately to verify that it does not exceed the worst case conditions specified for the specific system configuration. The measurements are performed a number of times to determine the statistical characteristics of each signal path.

BTP HICB-21, "Guidance on Digital Computer Real-Time Performance," states that digital system architecture affects the performance because communication between components of the system takes time, and allocation of functions to various system components affects timing. The architecture may also affect timing because an arrangement of otherwise simple components may have unexpected interactions. Specific timing requirements may affect the system architecture because it may not be possible to get sufficient computational performance for a specific function or group of functions from a single processor.

The staff has reviewed the TXS system architecture and the system response time test methodology as discussed in report EMF-2341(P) and found the TXS system design consistent with BTP HICB-21. It is, therefore, acceptable.

The protection system response time tests will be performed plant-specifically by licensees in accordance with plant technical specification requirements. The licensee must evaluate plant-specific accident analyses to confirm that a TXS reactor trip system (RTS) includes the provision to detect accident conditions and anticipated operational occurrences in order to initiate reactor shutdown (safety analysis confirmation for accuracy and time response) consistent with the accident analysis presented in Chapter 15 of the plant safety analysis report. This is a plant-specific action item.

4.4 Software Development Life Cycle

The software development life cycle used at Siemens for the TXS system is based on the waterfall life cycle described in various software development standards. The life cycle consists of the system specification phase, the functional specification phase, the detailed design description phase, the implementation phase, the test specification phase, and the test phase. The remaining phases (i.e., the integration phase and the operation and maintenance phase) are plant-specific. The licensee's plant-specific software development procedures must be equivalent to industry standards and practices endorsed by the NRC.

The adequacy of the Siemens development process was reviewed by the staff during an audit at the vendor facility. The staff conducted a life cycle process audit of the TXS by tracing three requirements through the software life cycle. The first audit of requirements conducted by the staff involved change request 200 (CR200), which implemented the S706 input/output driver, version 1.20. The staff reviewed the documentation supporting the life cycle phases of system specifications, functional specifications, detailed design specifications, implementation (by code review), test specifications, test results, and the certification update. In the review of the test specifications and the test results for consistency with test specifications, the staff concluded that the development of the S706 input/output driver was consistent with the Siemens software life cycle processes and, therefore, was acceptable.

The second audit of requirements conducted by the staff involved the 2.MIN function module life cycle processes. The purpose of this software module is to select a signal from a group of signals for subsequent use in a function group. The staff found one discrepancy in the ANSI C source codes in which the comment for one requirement was not changed when the CASE/SWITCH was changed to incorporate a DEFAULT-label in the source code. The discrepancy had been noted in the IV&V comments, but had not been incorporated into the module source code documentation because the change did not affect the function of the module. The correction to the comment has been listed as an action item for the next revision to the source code. The staff found the decision to delay action until the next revision to the source code to be appropriate. The staff suggested to Siemens that the Siemens coding guidelines should be followed for documentation as well as for actual coding. The rest of the source code documentation was consistent with the corresponding source code.

The third audit of requirements conducted by the staff involved CR203, which addressed the process by which data may be entered in a SPACE function block module diagram. The change was required to remove the capability to enter hardware-specific parameter information from the network diagram parameter entry dialog screen. The change request was processed according to Siemens procedures, following all of the Siemens requirements, including verification and validation.

The staff noted that Siemens does not have in place a requirements traceability matrix (RTM) for enumerating and tracking each system requirement throughout its life cycle. There are no standards that require the use of an RTM, but the practice of enumerating each requirement does assist in tracking requirements during future modifications. There was a discussion regarding the use of an RTM, and the possible creation of an RTM for future development efforts. There is no outstanding commitment or action item regarding this matter, however, the need for an RTM will be pursued as part of assessing future modifications on plant-specific applications of the TXS.

During the staff audit, the staff discussed the development history of the application-specific integrated circuit (ASIC) chip that is used for the system support controller (SSC) on the SVE1 central processor unit (CPU) board and on the SCP1 communication processor board. The SSC was developed approximately 10 years ago for general applications (not just the TXS) by another subsidiary of Siemens. Consequently, documentation of the SSC development was not available for review. On the basis of known broad usage, documented failure data, and ability to identify critical characteristics, Siemens commercially dedicated the SSC for applications in the TXS system.

There have been three SSC chip failures on VE286 and VE386 processor modules. These older modules were used in industrial automation computers of industries other than the nuclear power industry. Five years ago, the Siemens subsidiary that manufactures the SSC adopted a more detailed recording system to document failures. However, these three failures occurred more than five years ago and are not documented under the more detailed system that has been in place since 1994. The faults were identified as complete failures of the SSC chip as opposed to isolated internal logic anomalies. There has been no redesign of the SSC logic as a consequence of these faults. Siemens concluded that these initial three failures were random physical occurrences. The staff finds this conclusion acceptable.

The only failure recorded in 2688 nuclear industry applications was on an SVE1 module. Siemens determined that this failure was caused by a soldering defect at one of the pins of the SSC and was not a failure of the SSC chip itself. The staff, therefore, finds the commercial dedication of the SSC chip to be acceptable.

The staff reviewed the Siemens configuration management process to confirm that various versions of documentation are properly controlled, and did not identify any discrepancies.

On the basis of its review of the software processes used throughout the software life cycle, and on the basis of its audit of software development documentation, the staff concludes that the software development process used at Siemens is acceptable.

The independent verification and validation (IV&V) process for the Siemens TXS is consistent with the IV&V process described in IEEE 1012-1998. Two organizations (iSTec and TÜV Nord) perform IV&V activities through a contract with the GRS. These two organizations report their findings to GRS and to Siemens, and also provide formal certification for each product. If a certified product requires modification, the modified product is submitted to iSTec or TÜV Nord for IV&V for a new certification. The staff concludes that the Siemens IV&V effort is sufficiently independent in personnel, management, and financial resources.

The IV&V processes address all phases of the Siemens software life cycle up to the testing of plant-specific applications. The staff did not address plant-specific applications of IV&V activities, as these activities were not in the scope of the staff review.

On the basis of its review of the Siemens engineering procedures and the results of its audit of Siemens software development processes, the staff concludes that Siemens has an acceptable software development methodology and follows this methodology consistently in developing safety-related software. The staff also determines that SPACE (specification and coding environment) tool for designing and assembling safety-related applications has the capability and safeguards to ensure that the implementation of the application programs can be successfully accomplished on a plant-specific basis.

5.0 SUMMARY OF REGULATORY COMPLIANCE EVALUATIONS

This safety evaluation discussed the acceptability of the TXS system. The general design criteria (GDC) listed in 10 CFR Part 50 Appendix A establish minimum requirements for the design of nuclear power plants. IEEE-603 is also incorporated in 10 CFR 50.55a(h). The regulatory guides and the endorsed industry codes and standards listed in NUREG-0800, "Standard Review Plan," Table 7-1, are the guidelines used as the basis for this evaluation.

Three Mile Island (TMI) Action Plan requirements for I&C systems are also identified in Table 7-1 of the SRP. Siemens has used a number of German standards in addition to the standards listed in the SRP.

Section 50.55a(a)(1) of Title 10 of the Code of Federal Regulations (10 CFR), "Quality Standards for Systems Important to Safety", is addressed by conformance with the codes and standards listed in the SRP. Siemens uses codes and standards in the development of the TXS system that are the same as or equivalent to the standards in the SRP and, therefore, the TXS system is in conformance with this requirement.

Section 50.55a(h) of 10 CFR endorses IEEE-603, which addresses both system level design issues and quality criteria for qualifying devices. Siemens has addressed these issues in the topical report. The TXS system meets the criteria of IEEE-603 and the supplemental standard IEEE-7-4.3.2-1996. The staff concludes, therefore, that the TXS system is in compliance with this requirement.

Section 50.34(f)(2)(v) of 10 CFR, "Bypass and Inoperable Status Indication (TMI Action Plan Item 1.D.3)," has been addressed in the TXS system design and is, therefore, in conformance with this requirement.

Section 50.34(f)(2)(xii) of 10 CFR, "Auxiliary Feedwater System Automatic Initiation and Flow Indication (TMI Action Plan Item II.E.1.2)," is a plant system requirement and is not specifically addressed in the topical report; however, the TXS system has the capability of meeting this requirement. Plant-specific application should demonstrate the compliance with this requirement.

Section 50.34(f)(2)(xvii) of 10 CFR, "Accident Monitoring Instrumentation (TMI Action Plan Item II.F.1)," has sampling and analyzing requirements. The TXS system is capable of providing plant process data for the display portion of this requirement. Plant-specific application should demonstrate the compliance with this requirement.

Section 50.34(f)(2)(xviii) of 10 CFR, "Instrumentation for the Detection of Inadequate Core Cooling (TMI Action Plan Item II.F.2)," is not specifically addressed in the topical report; however, the TXS system is capable of meeting the processing and display portions of this requirement. If an inadequate core cooling detection system is supported by the TXS system, then a plant-specific application should demonstrate the compliance with this requirement.

Section 50.34(f)(2)(xiv) of 10 CFR, "Containment Isolation Systems (TMI Action Plan Item II.E.4.2)," is not specifically addressed in the topical report; however, the TXS is capable of meeting the processing and display portions of this requirement. A plant-specific application should demonstrate the compliance with this requirement.

Section 50.34(f)(2)(xix) of 10 CFR, "Instrumentation for Monitoring Plant Conditions Following Core Damage (TMI Action Plan Item II.F.3)," is not specifically addressed in the topical report; however, the TXS is capable of meeting the processing and display portions of this requirement. A plant-specific application should demonstrate the compliance with this requirement.

Section 50.34(f)(2)(xx) of 10 CFR, "Power for Pressurizer Level Indication and Controls for Pressurizer Relief and Block Valves (TMI Action Plan Item II.G.1)," requires that the indicators continue to operate during a loss of offsite power. The TXS system is capable of providing the indication and controls. A plant-specific application should demonstrate the compliance with this requirement.

Section 50.34(f)(2)(xxiv) of 10 CFR, "Central Reactor Vessel Water Level Recording (TMI Action Plan Item II.K.3.23)," requires that reactor vessel water level be monitored during post-accident conditions. The TXS system can satisfy this requirement. A plant-specific application should demonstrate the compliance with this requirement.

Section 50.62 of 10 CFR, "Specifies Requirements for Reduction of Risk from Anticipated Transients Without Scram (ATWS)." The TXS system is acceptable for the ATWS mitigation system; however, the reactor protection system would have to be diverse from the ATWS mitigation system. Consequently, if a licensee develops an ATWS mitigation system based on the TXS system, the licensee must show that the system is diverse from the reactor protection system to receive staff approval.

The following 10 CFR Part 50, Appendix A, general design criteria are the applicable design criteria for this review:

- Criterion 1 - quality standards and records
- Criterion 4 - environmental and missile design bases
- Criterion 13 - instrumentation and control
- Criterion 20 - protection system functions
- Criterion 21 - protection system reliability and testability
- Criterion 22 - protection system independence
- Criterion 23 - protection system failure modes
- Criterion 24 - separation of protection and control systems

The following regulatory guides (RGs) are applicable to this review:

- RG 1.22, "Periodic Testing of Protection System Actuation Functions"
- RG 1.47, "Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems"
- RG 1.62, "Manual Initiation of Protection Action"
- RG 1.75, "Physical Independence of Electrical Systems"
- RG 1.97, "Instrumentation for Light-Water-Cooled Nuclear Power Plants to Assess Plant and Environs Conditions During and Following an Accident"
- RG 1.118, "Periodic Testing of Electric Power and Protection Systems"
- RG 1.152, "Criteria for Digital Computers in Safety Systems of Nuclear Power Plants"
- RG 1.153, "Criteria for Power Instrumentation and Control Portions of Safety Systems"

- RG 1.168, "Verification, Validation, Reviews and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants"
- RG 1.169, "Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants"
- RG 1.170, "Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants"
- RG 1.171, "Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants"
- RG 1.172, "Software Requirements Specification for Digital Computer Software Used in Safety Systems of Nuclear Power Plants"
- RG 1.173, "Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants"

SRP Section 7.1-C provides guidance for evaluation of conformance to IEEE-603. IEEE-603 provides criteria for I&C systems in general. Reference is made to IEEE-7-4.3.2 for hardware and software issues of digital computers.

To meet the single-failure criterion for U.S. applications, the TXS is applied to four redundant process channels and two trip logic trains for each RPS or ESF actuation function. These redundant channels and trains are electrically isolated and physically separated. Qualified isolation devices have been tested to ensure functional operability when subjected to physical damage, short circuits, open circuits, or credible fault voltages on the device output terminals.

The completion of protective action requirement has been satisfied. Once initiated with the TXS system, the RPS and ESF actuations proceed to completion. Return to normal operation requires deliberate operator action to reset the reactor trip breakers. The reactor trip breakers cannot be reset while a reactor trip signal is present in the safety system. ESF actuations proceed to completion unless deliberate operator action is taken to terminate the function. The design is implemented consistent with plant specific functional logic to enable system-level protective actions to proceed to completion.

The quality criterion is satisfied with the Siemens Power Corporation Quality Assurance Program that meets the requirements of 10 CFR Part 50, Appendix B.

TXS is environmentally and seismically qualified to ensure the system is capable of performing its designated functions while exposed to normal, abnormal, test, accident and post-accident environmental conditions. The type testing was performed in accordance with KTA-3503. Mild environment qualification conforms to the guidance of IEEE-323, "IEEE Standard for Qualifying Class IE Equipment for Nuclear Power Generating Stations." EMC has been verified in accordance with the IEC-61000 standards. However, plant-specific environmental, seismic, and EMI qualification will be retested to be consistent with the guidance of EPRI TR-107330, and TR-102323, as stated in Sections 2.1.2.1, 2.1.2.2 and 2.1.2.3 of this report.

The independence criterion in the TXS system is met through the redundancy and separation of the channels. The communication between channels is via fiber optic cable.

The capability for testing and calibration has been demonstrated in compliance with RG 1.22, RG 1.118, and IEEE-338. The capability exists to permit testing during power operation. The design does not require disconnecting wires, installing jumpers, or other similar modifications of the installed equipment.

Access to the hardware is controlled via the front and rear cabinet doors, which are normally locked. Door positions are monitored, with an alarm to the operator if any door is opened.

The human factors considerations will be evaluated on a plant-specific basis and, therefore, are not included in this review.

Reliability has been assessed with both probabilistic and deterministic reliability analyses. The probabilistic analysis has been used to quantify the nonavailability on demand. The staff has reviewed these calculations; however, the staff does not use probabilistic and deterministic reliability analyses as the sole means of determining acceptability of a safety system. The calculations are related only to the hardware aspects of the TXS system; however, confirmatory testing performed by Siemens and GRS included the software. The deterministic analysis based on codes and standards delineates postulated failures that the system will be able to withstand.

The TXS meets the automatic and manual control requirements. Failure of the automatic controls does not interfere with the manual controls.

Setpoints will be evaluated on a plant-specific basis. The licensee must ensure that, when the TXS system is installed, overly conservative setpoints due to the elimination of analog system drift are not retained, as this would increase the possibility that the TXS equipment may be performing outside the vendor specifications.

The NRC staff concludes that the design of the TXS safety systems meets the relevant requirements of General Design Criteria (GDC) 1, 2, 4, 13, 19-25, and 29, and 10 CFR 50.34(f), 10 CFR 50.55a(a)(1), and 10 CFR 50.55a(h), and is, therefore, acceptable.

The staff conducted a review of the safety system descriptions in the topical report for conformance to the guidelines in the regulatory guides and industry codes and standards applicable to these systems. The staff concludes that the applicant adequately identified the guidelines applicable to these systems. Based upon the review of the safety system designs for conformance to the guidelines, the staff finds that there is reasonable assurance that the TXS system conforms to the guidelines applicable to these systems. Therefore the staff finds that the requirements of GDC 1 and 10 CFR 50.55a(a)(1) have been met.

The review included the identification of those systems and components for the safety systems designed to survive the effects of earthquakes, other natural phenomena, abnormal environments, and missiles. On the basis of this review, the staff concludes that the applicant has identified those systems and components consistent with the design bases for those systems. Therefore, the staff finds that the identification of these systems and components satisfies the requirements of GDC 2 and 4.

Based on the review of safety system status information, manual initiation capabilities, and provisions to support safe shutdown, the staff concludes that information is provided to monitor the safety systems over the anticipated ranges for normal operation, for anticipated operational occurrences, and for accident conditions so as to ensure adequate safety. Appropriate controls are provided for manual initiation of a reactor trip. The TXS safety systems appropriately support actions to operate the nuclear power unit safety under normal conditions and to maintain it in a safe condition under accident conditions. Therefore, the staff finds that the TXS system designs satisfy the requirements of GDC 13 and 19.

Based on the review of system functions, the staff concludes that a TXS system conforms to the design bases requirements of IEEE Std 603 and 10 CFR 50.34(f) and to the guidance of RG 1.105. On the basis of its review, the staff concludes that the TXS includes the provision to detect accident conditions and anticipated operational occurrences in order to initiate reactor shutdown consistent with the accident analysis presented in Chapter 15 of the plant's Safety Analysis Report (SAR). Licensee evaluation of plant-specific accident analyses is required. Therefore, the staff finds that the TXS satisfies the requirements of GDC 20.

The TXS system conforms to the guidelines for periodic testing in RG 1.22 and RG 1.118. The bypassed and inoperable status indication conforms to the guidelines of RG 1.47. The safety systems conform to the guidelines on the application of the single-failure criterion in ANSI/IEEE Std 379, as supplemented by RG 1.53. On the basis of this review, the staff concludes that the TXS system satisfies the requirement of IEEE-603 with regard to system reliability and testability. Therefore, the staff finds that the TXS system satisfies the requirements of GDC 21.

The TXS system conforms to the guidelines in RG 1.75 for protection system independence. On the basis of its review, the staff concludes that the TXS system satisfies the requirement of IEEE-603 with regard to system independence. Therefore, the staff finds that the TXS system satisfies the requirements of GDC 22.

On the basis of its review of the failure modes and effects analysis for the TXS system, the staff concludes that the systems are designed to fail into a safe mode if conditions such as disconnection of the system, loss of energy, or adverse environment are experienced. Therefore, the staff finds that the TXS system satisfies the requirements of GDC 23.

Based on its review of the interfaces between the TXS safety systems and plant operating control systems, the staff concludes that the TXS safety systems satisfy the requirements of IEEE-603 with regard to control and protection system interactions. Therefore, the staff finds the TXS safety systems satisfy the requirements of GDC 24.

On the basis of its review of all the above GDCs, the staff concludes that the TXS system satisfies the requirements of GDC 29, "Protection Against Anticipated Operational Occurrences."

The staff's conclusions are based upon the requirements of ANSI/IEEE-603 with respect to the design of the TXS system. Therefore, the staff finds that the TXS system satisfies the requirement of 10 CFR 50.55a(h) with regard to ANSI/IEEE-603.

On the basis of its review of the Siemens defense-in-depth and diversity analysis methodology, the staff concludes that licensees implementing this methodology will comply with the criteria for defense against common-mode failure in digital instrumentation and control systems. Therefore, the staff finds that adequate diversity and defense against common-mode failure will be provided to satisfy these requirements of GDC 21 and 22 and Item II.Q of the staff requirements memorandum of SECY-93-087. The staff requires, however, that each licensee ensure that the plant-specific application complies with the criteria for defense against common-mode failures in digital instrumentation and control systems.

On the basis of its review of software development plans and inspections of the computer development process and design outputs, the staff concludes that the TXS safety systems meet the guidance of RG 1.152. Therefore, the special characteristics of computer systems have been adequately addressed, and the staff finds that the TXS system satisfies the requirements of GDC 1 and 21.

The staff concludes that the TXS system meets the requirements of 10 CFR Part 50, Appendix A General Design Criteria 1, 2, 4, 13, 19-24, and 29, and IEEE-603 for the design of safety-related reactor protection systems, engineered safety features systems, and other plant systems, and the guidelines of Regulatory Guide 1.152 and supporting industry standards for the design of digital systems and is, therefore, acceptable.

The design principle for software of Class 1E systems is to ensure that the sequence of processing executed for each expected situation can be deterministically established. It discourages the use of non-deterministic data, communications, non-deterministic computations, multitasking, dynamic scheduling, use of non-deterministic interrupts and event-driven designs. Based on its review, the staff determines that the design of the TXS system satisfies this design principle for Class 1E system software.

6.0 PLANT-SPECIFIC ACTION ITEMS

On the basis of the above review, the staff concludes that the TXS system is acceptable for use in the development, installation and operation of safety-related systems in nuclear power plants, subject to the following conditions:

The following actions must be performed by an applicant when requesting NRC approval for installation of a Siemens TXS system:

1. The licensee must demonstrate that the generic qualification bounds the plant specific condition (i.e., temperature, humidity, seismic, and electromagnetic compatibility) for the location(s) in which the TXS equipment is to be installed. The generic qualification data must comply with EPRI qualification requirements specified in EPRI TR-107330 and TR-102323-R1 (see Sections 2.1.2.1, 2.1.2.2, and 2.1.2.3).
2. The licensee's plant-specific software development V&V activities and configuration management procedures must be equivalent to industry standards and practices endorsed by the NRC (as referenced in SRP BTP HICB-14, "Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems") (see Sections 4.4, 2.2.3, 2.2.4).

3. If the licensee develops a TXS auxiliary feedwater control system, the licensee must include automatic initiation and flow indication (TMI Action Plan Item II.E.1.2). The licensee needs to confirm that the plant-specific application conforms to the requirements of 10 CFR 50.34 (f)g(2)(xii) (see Section 5.0).
4. If the licensee replaces existing accident monitoring instrumentation (TMI Action Plan Item II.F.1) display capabilities with a TXS system, including the bypass and inoperable status information, the licensee needs to confirm that the new system provides equivalent sampling and analyzing features, and meets the requirement of 10 CFR 50.34 (f)(2)(xvii) (see Section 5.0).
5. If the licensee installs a TXS inadequate core cooling detection system, the licensee needs to confirm that the new system conforms to the requirements of 10 CFR 50.34(f)(2)(xviii) (see Section 5.0).
6. If the licensee installs a TXS containment isolation system (TMI Action Plan Item II.E.4.2), the licensee must verify that the plant-specific application conforms to the requirement of 10 CFR 50.34 (f)(2)(xiv) (see Section 5.0).
7. For monitoring plant conditions following core damage, the licensee must verify that the TXS system meets the processing and display portions of the requirements of 10 CFR 50.34(f)(2)(xix) (see Section 5.0).
8. If the licensee installs a TXS system for monitoring reactor vessel water level during post -accident conditions, the licensee must provide plant-specific verification of the ranges, and confirm that human factors issues have been addressed, as required by 10 CFR 50.34(f)(2)(xxiv) (see Section 5.0).
9. If the licensee installs a TXS reactor protection system, the licensee must provide confirmation that the TXS system is diverse from the system for reducing the risk from anticipated transients without scram (ATWS), as required by 10 CFR 50.62. If the licensee installs a TXS ESFAS, the licensee must provide confirmation that the diversity requirements for plant systems (feedwater, auxiliary feedwater, turbine controls, etc.) are maintained (see Section 5.0).
10. Setpoints will be evaluated on a plant-specific basis. The licensee must ensure that, when the TXS system is installed, overly conservative setpoints that may occur due to the elimination of analog system drift are not retained, as this would increase the possibility that the TXS equipment may be performing outside the vendor specifications. The licensee must provide the staff with a revised setpoint analysis that is applicable to the installed TXS system(s) (see Section 4.4).
11. The licensee must evaluate plant-specific accident analyses to confirm that a TXS reactor trip system (RTS) includes the provision to detect accident conditions and anticipated operational occurrences in order to initiate reactor shutdown (safety analysis confirmation for accuracy and time response) consistent with the accident analysis presented in Chapter 15 of the plant safety analysis report (see Section 4.3).

12. The staff requires that each licensee ensure that the plant-specific TXS application complies with the criteria for defense against common-mode failures in digital instrumentation and control systems (see Section 4.1).
13. The licensee should propose plant-specific Technical Specifications including periodic test intervals (see Section 4.2).
14. The licensee should demonstrate that the power supply to the TXS system complies with EPRI TR-107330 requirements (see Section 2.1.2.4).
15. The licensee should demonstrate that the qualification of the isolation devices were performed in accordance with EPRI TR-107330 requirements (see Section 2.1.3).
16. The licensee should demonstrate that Siemens TXP (control systems) or other manufacturer's control systems satisfy the acceptance guidance set forth in Section 4.1 of this safety evaluation (see Section 4.1).
17. The licensee should address the need for a requirement traceability matrix (RTM) for enumerating and tracking each system requirement throughout its life cycle, particularly as part of making future modifications (see Section 4.4).

Principal Contributors: E. Lee
M. Waterman
H. Li

Date: May 5, 2000