Oconee Plant Protection System Digital Replacement Project:

Technical Discussions for Selected Safety System Topics

Mark Burzynski
Sean Kelley
Dr. Steffen Richter

Introduction

Mark Burzynski

Meeting Objectives

> Provide an overview of the Oconee digital plant protection system

> Provide technical discussion of key elements of the Oconee digital plant protection system (PPS)

> Provide detailed technical discussion of key aspects of the TELEPERM XS™ regarding communication independence

Meeting Outline

> Introduction and Background (Mark Burzynski)

> Oconee System Overview (Sean Kelley)

> Communication Networks and Isolation Schemes (Sean Kelley)

> Communication Processing (Dr. Steffen Richter)

> Interchannel Communication (Sean Kelley)

> Communication with Service Unit (Dr. Steffen Richter)

> Communication via Gateway (Dr. Steffen Richter)

> Regulatory Analysis (Robert Gill)

Introduction

- TXS computer processors use a deterministic operating system
  - Increases the predictability of the software
- The most important features of the TXS software design include a strictly cyclic processing of application software
  - Asynchronous operating system (meaning no real-time clock that redundant processors synchronize to) reduces failure potential and enhances reliability
- Only static memory allocation is used
  - Each variable in the application program has a permanent dedicated place in memory, so that memory conflicts caused by dynamic memory allocation are not possible
- There is a complete absence of process-driven interrupts
- Other important features include:
  - Bus systems with a constant load
  - No long-term data storage
  - No use of external data storage media.

Potential for software failure is minimized by deterministic operating system built high-quality software design tools

Background

- The TELEPERM XS system is fully described in Topical Report EMF-2110, Revision 1, "TELEPERM XS: A Digital Reactor Protection System," September 1, 1999
- NRC issued a safety evaluation report for the topical report
  - Letter dated May 5, 2000, from Stuart A. Richards, NRC, to Jim Mallay, Siemens Power Corporation, 'Acceptance for Referencing of Licensing Topical Report EMF-2110 (NP), Revision 1, "TELEPERM XS: A Digital Reactor Protection System"

AREVA

Background

> The safety evaluation report concluded that

"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 1 E system software."

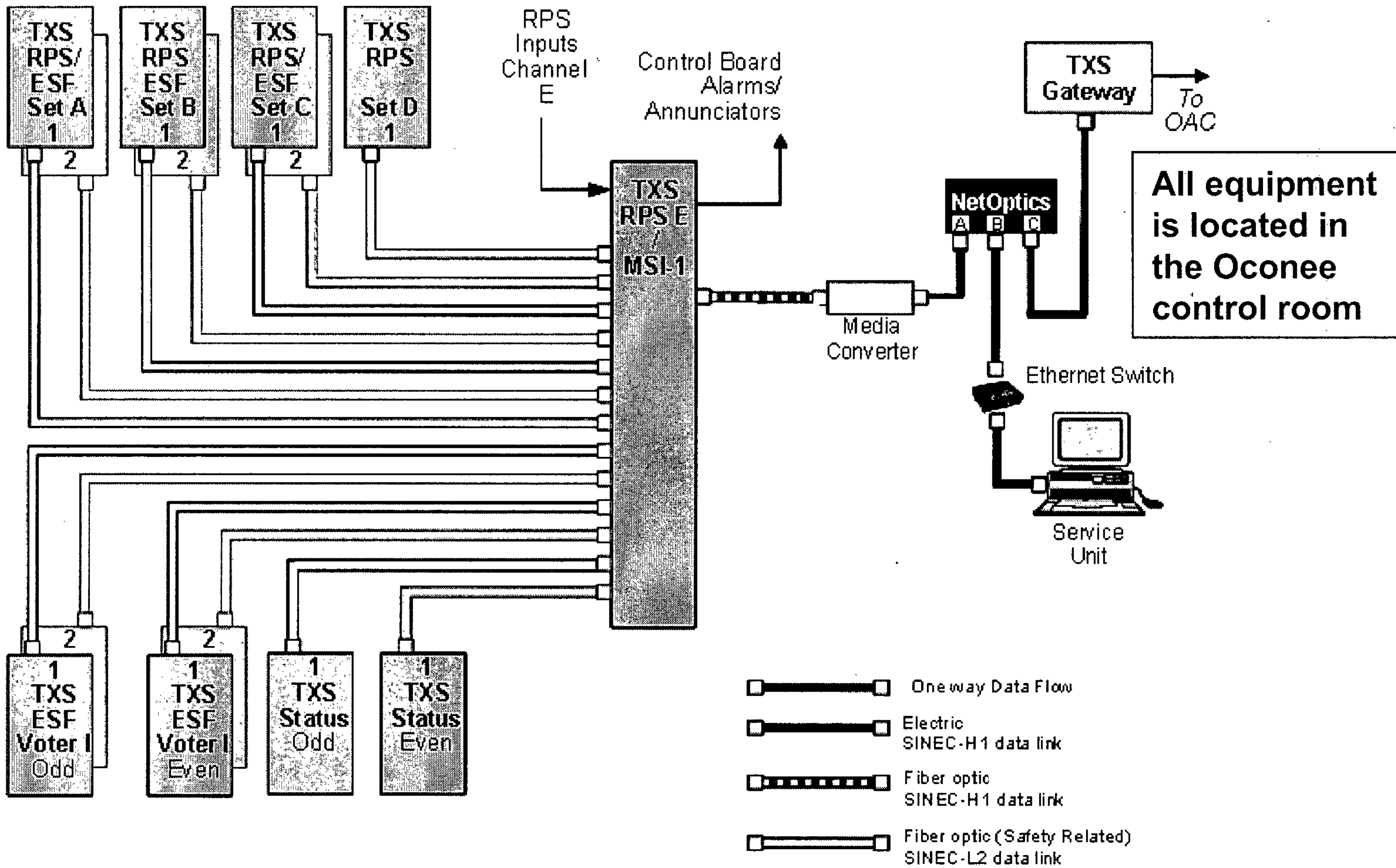
"The staff's conclusions are based upon the requirements of ANSI/IEEE-603 with respect to the design of the TXS system. Therefore, the staff finds that the TXS system satisfies the requirement of 10 CFR 50.55a(h) with regard to ANSI/IEEE-603."

Presentation today will review the TXS communication independence features regarding compliance with IEEE 603 – 1991 and applicable regulatory guidance

Oconee Protection System and TELEPERM XS™ Overview

Sean Kelley

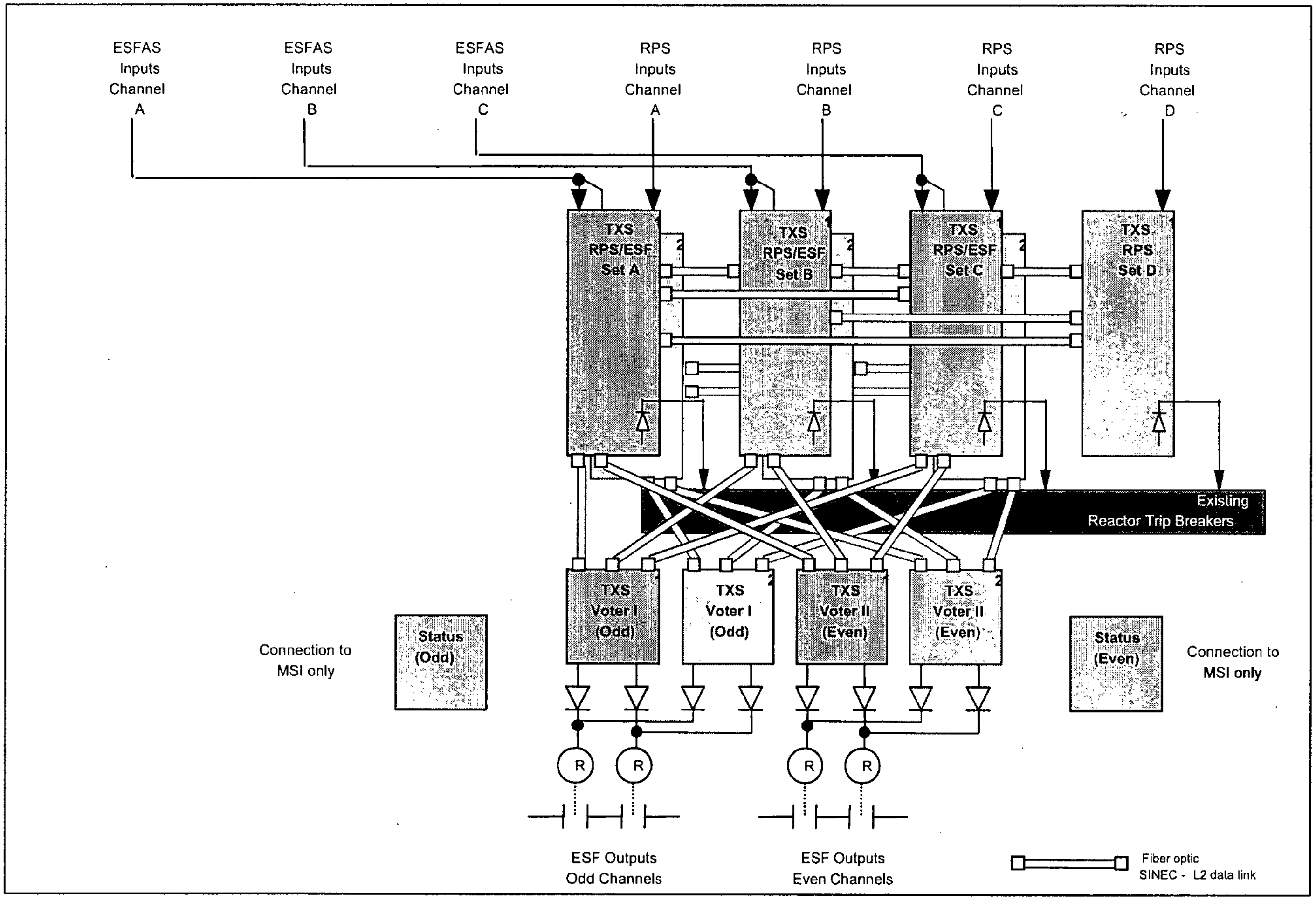
Oconee PPS Architecture



All equipment is located in the Oconee control room

Network Architecture of the New Oconee PPS

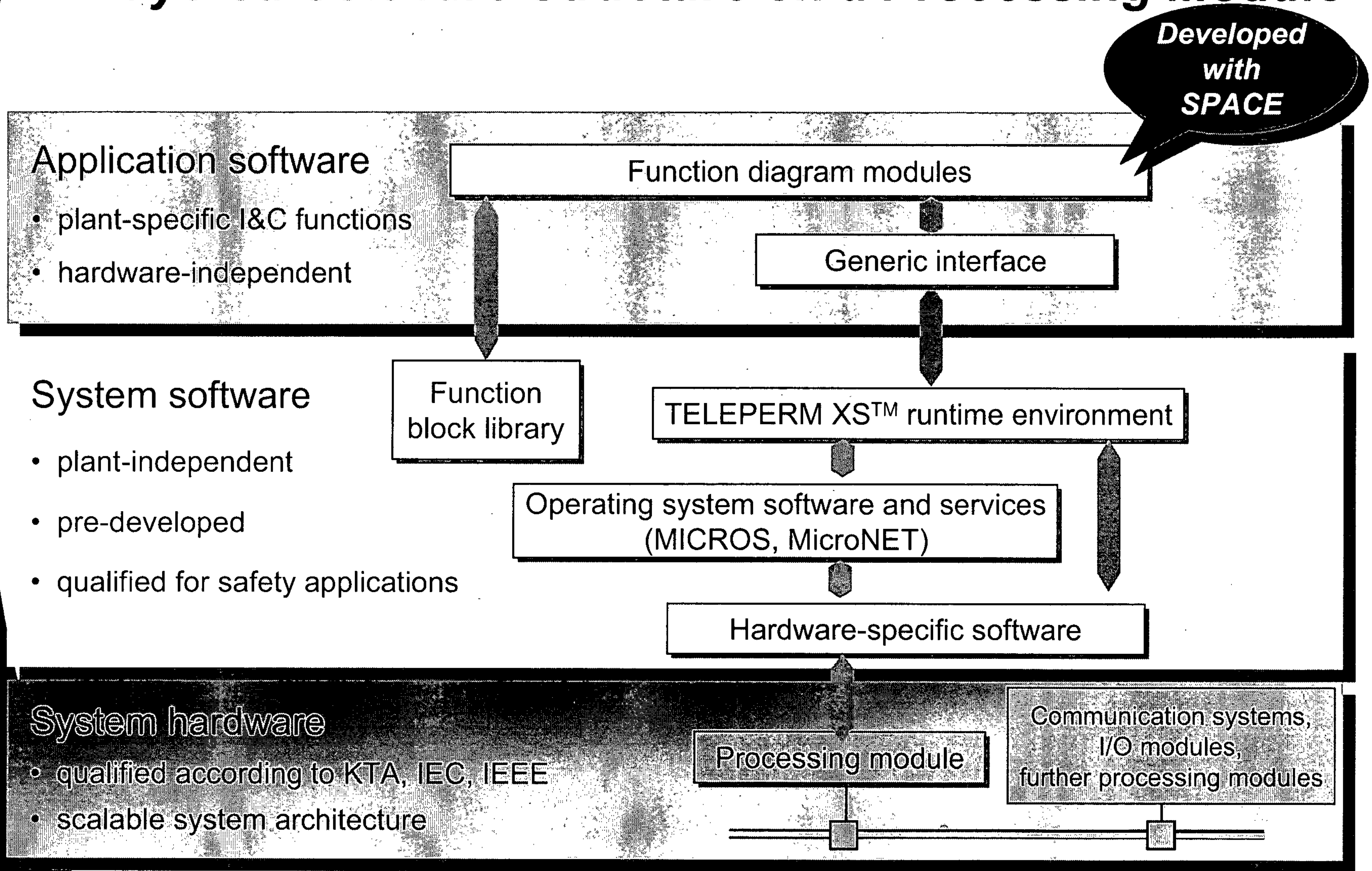
Oconee PPS Architecture



Oconee PPS Interchannel Communication Architecture

TELEPERM XS™ System Platform Architecture

Layered Software Structure on a Processing Module



RTE Configuration Module

> "Generic interface" between I&C application and system software

> Generated by the SPACE code generator individually for each CPU

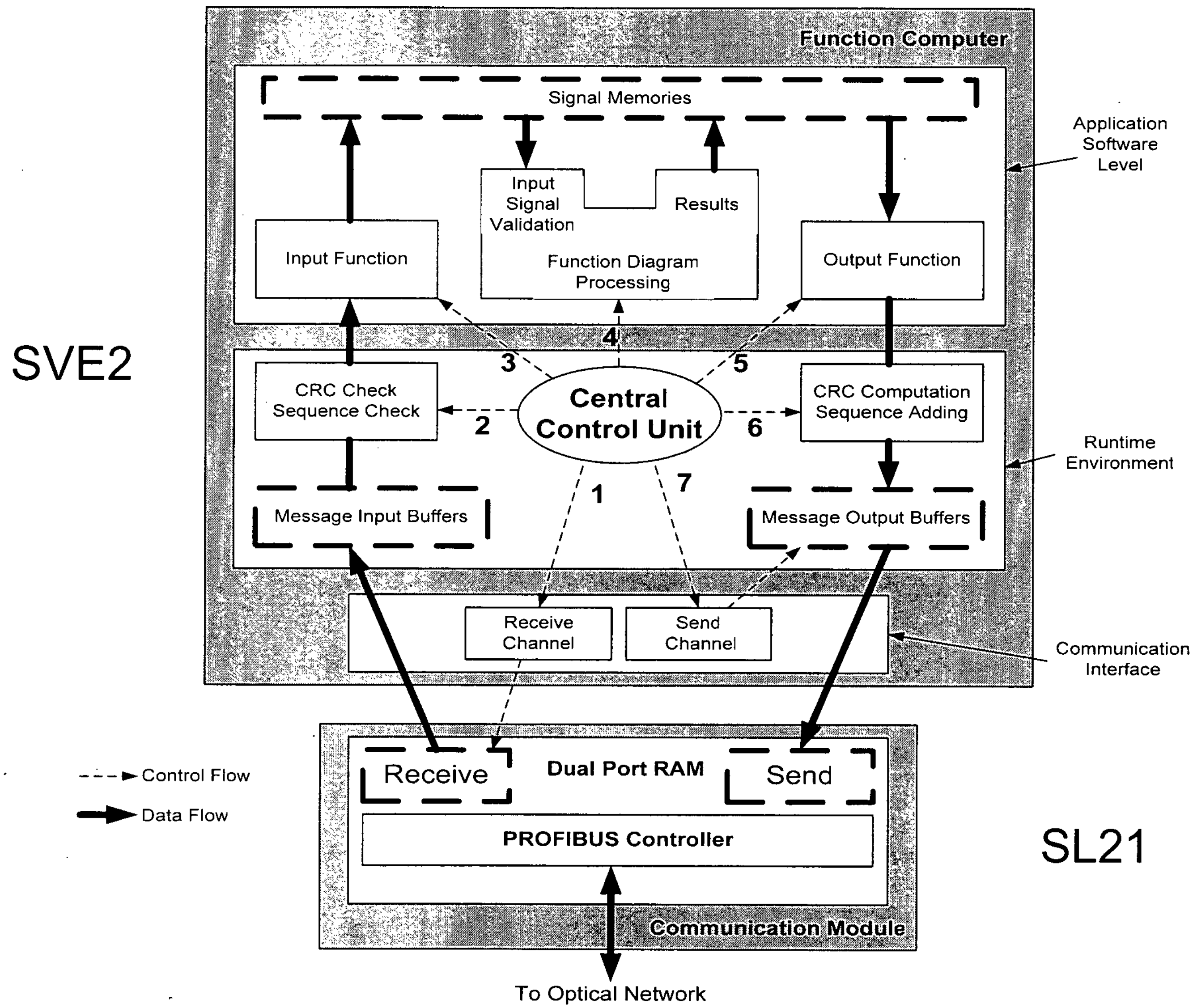
> Comprises parameters for RTE and various data structures/arrays needed to describe:

- a unique processor ID (CPU ID) for the processing module
- the operating and communication cycle times
- the entry points and interface data to the FDG modules to be processed
- all configuration data for the input/output (I/O) drivers
- the complete lists of all messages to be sent or received by the RTE and communication channel parameters

Role of Runtime Environment

- Unified software environment for the processing modules used for the execution of the TXS application software (FDG modules)
- Hides all target system specifics from the FDG modules (hardware, operating system, communication media and protocols, I/O modules, etc.)
- Central control instance for
  - Cyclic processing of the FDG modules
  - Signal transfers via messages or directly by I/O modules
- Provides the interface of the system software with the TXS Service Unit for monitoring and servicing
  - Tracing signal data, reading error messages, switching operation modes, adjusting parameterization of FB modules

TXS Safety Classified Communication: Processing Overview



TXS Safety Classified Communication: Processing Overview

> Central Control Unit coordinates data flow in a sequential fashion:
  1) Communication interface transfers messages from "receive RAM" to corresponding message input buffers
  2) CRC checksum, message identification and sequence increment checks performed and transfer of messages from message input buffers to input function
  3) Input function identifies individual signals within messages and allocates them to signal memories

TXS Safety Classified Communication: Processing Overview

4) Function diagram processing (including signal validation) is performed. Results stored in dedicated signal memory locations
5) Output function collects result signals and forms output messages.
6) RTE attaches new CRC checksum, message identification and cycle counter and stores messages in message output buffers
7) Communication interface transfers messages from message output buffers to "send RAM"

TXS Safety Classified Communication: Processing Summary

- Runtime environment controls all processing actions and ensures discrete, cyclic processing
- Independent control flow of function computer and communication module
- Token passing protocol used at communication module level to avoid data collisions
- Individual memory locations for each message ensure separation of send and receive flows
- Checks performed on received messages (prior to function diagram processing) ensure valid message transmission
- Checks on input signals ensure valid input data to function diagrams

System design ensures interference-free communication

AREVA

TELEPERM XS™ Communication Networks and Isolation Schemes

Sean Kelley

TXS Safety Classified Communication: Network Configurations

> Communications between safety function channels or between different cabinets in the same safety function channels use fiber optic cabling and optical link modules
> TXS platform provides multiple options for reliable network configurations
> Configurations selected based on specific applications

Selected network configurations ensure high network reliability

TELEPERM XS™ Communication
Types of Communication Buses

> TXS backplane bus (K32)

- 32 bit parallel bus in the TXS sub-rack
- Up to 8 communicating CPUs (SVE or SCP)
- Maximum data package size is 8192 bytes

Communication
... inside TXS computer units

> TXS PROFIBUS® (L2) network

- 1.5 Mbit/sec optical (RS422) token bus
- Maximum data package size is 244 bytes

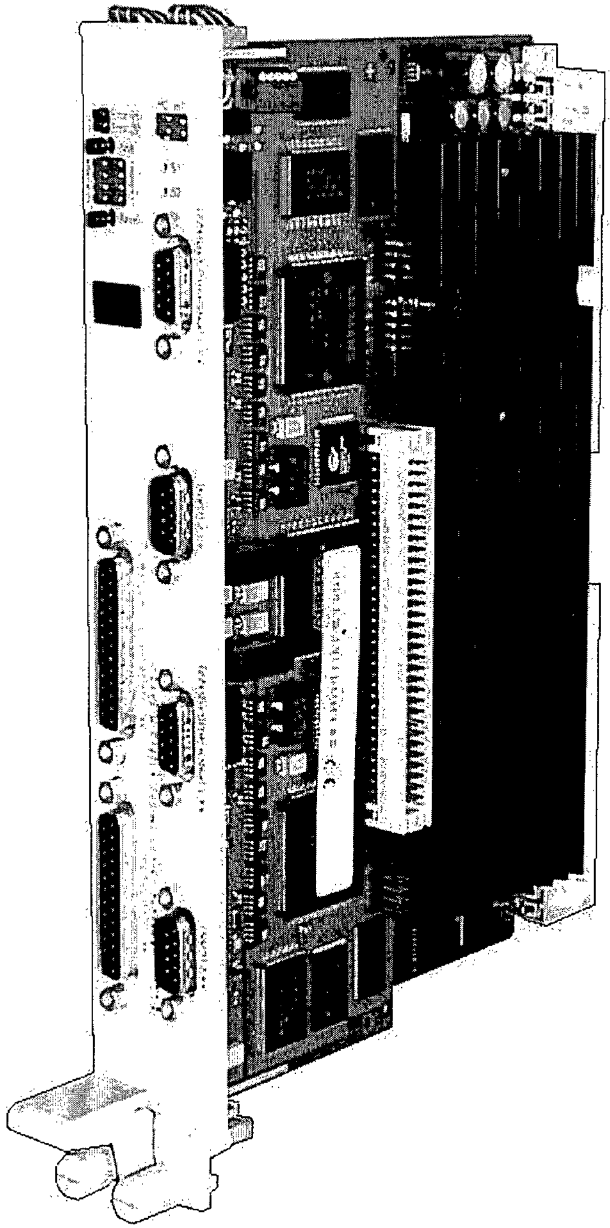
... between TXS computer units

> TXS Ethernet (H1) network

- 10 Mbit/sec optical bus, CSMA/CD according to IEEE 802.3
- Point-to-point or switch connections
- Maximum data package size is 1536 bytes

... with gateway and Service Unit

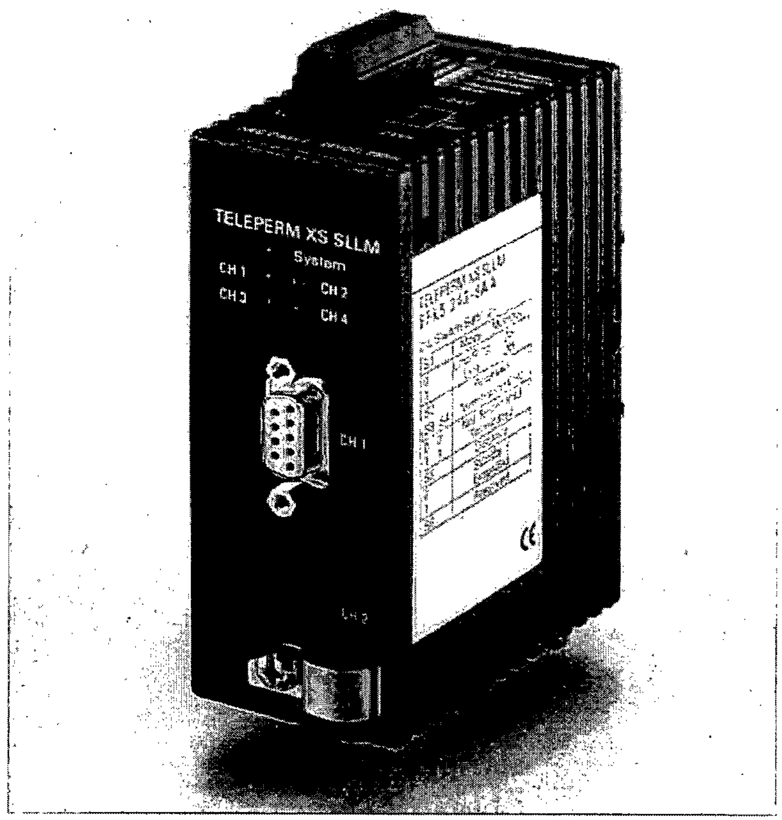
SVE2 + TXS PROFIBUS® (L2) module SL21



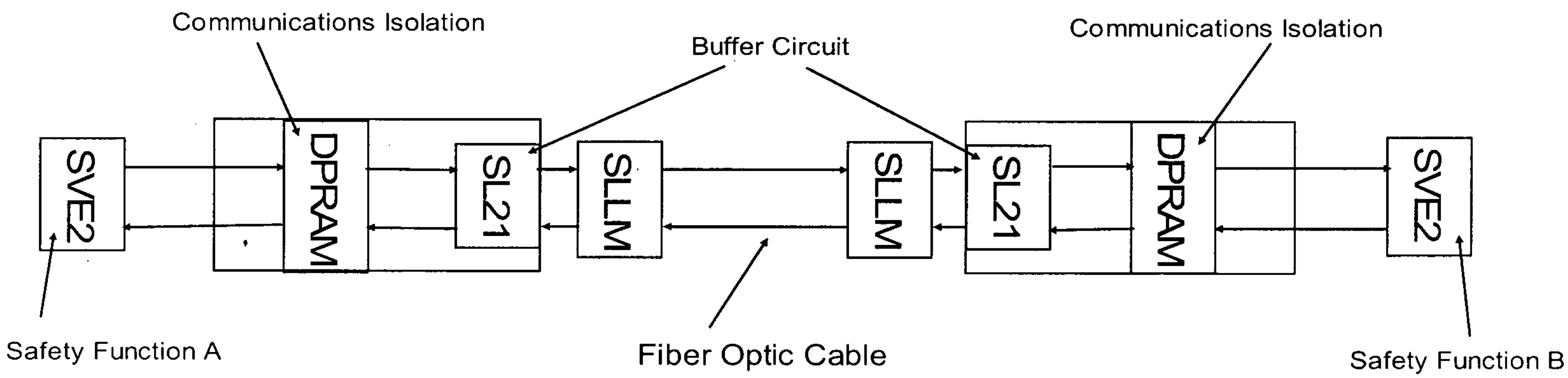
TXS Safety Classified Communication: Optical Link Modules

> Each link module contains electrical and optical channels
  - Only optical channels are used for safety related connections between different cabinets or divisions

> Link modules actively monitor optical paths for interruption
  - Monitoring achieved through "echo" functions
  - Faults in link modules or in optical paths are indicated locally and signaled to cabinet monitoring modules



Communication Independence



ES/RPS – Communication between safety channels and with MSI
(Two-way communication)

Oconee Communication Isolation Design

IEEE 7-4.3.2 Communication Independence

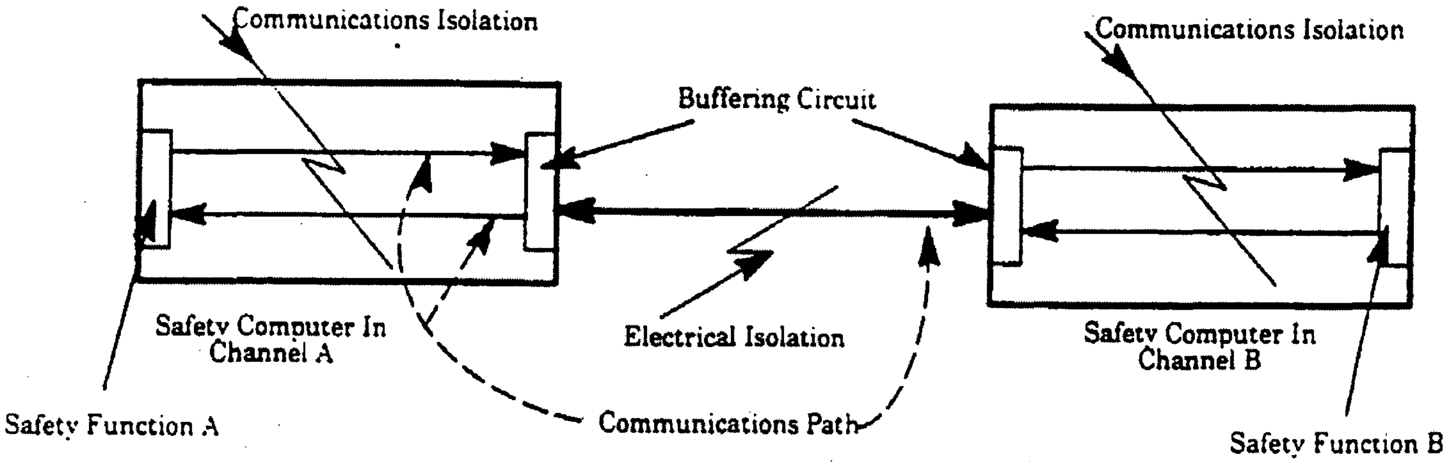


Figure G2—Communication between safety channels (Two-way communication)

IEEE Standard 7-4.3.2 Annex G Communication Isolation Guidance

TELEPERM XS™
Communication Processing

Dr. Steffen Richter

TELEPERM XS™ Communication Basic Principle

> Communication protocol does not use acknowledges by the receiver
  - Deterministically excluded that the receiver of a message can have any influence on the sender's operation

> Likewise, the sender cannot influence the operation of the receiver
  - Receiver can only act on the data in accordance with the function application software

Operating Principles

> Strictly cyclic signal processing
> No synchronization between processing modules (CPUs)
> Cyclic data transfer via network connections
  - Predefined package size
  - Constant bus load
  - Checksum and message age monitoring
> No dynamic allocation of resources
> Program code executed from Flash EPROM
> Parameter data stored in RAM and EEPROM (power-fail safe)
> Simple type of multi-tasking to handle background activities
  - Cyclic self-test
  - Response to service commands from Service Unit

TELEPERM XS™ Operation
Strictly Cyclic Processing

Cyclic Signal Processing

Interference-free Communication between TXS Units

Characteristics

> Application of a fiber optic transmission medium
  - Effects caused by electromagnetic interference cannot propagate

> Individual DPRAM buffers for each message
  - Separation of the data flow for sending and receiving

> Cyclic processing of all application and communication functions, including message transmission
  - Avoidance of mechanisms influencing the linked communication systems, independent control flow of communication modules and processing modules

> Check on all received messages
  - Message authentication, validity check and message age monitoring

> Not-a-number checking on all analog data received through data messages
  - Prevention of float exception due to input data

> On-line validation of input data in the TXS application software
  - Limits the propagation of faulty data
  - Provides valid input data for the subsequent function diagram module processing

TXS PROFIBUS® Communication Module SL21

- SL21 modules transfer data without influencing the message data.
- Sender side:
  - Performs an automatic polling cycle on message buffers of the DPRAM to recognize that new messages are stored there
  - In parallel, it waits for receiving the token (according to the token passing principle)
  - Reception of token equals permission to put data on the bus
  - After sending messages (if some), token is forwarded to the next SL21 on the bus (round robin)
- Receiver side:
  - Listens to the bus, receives data messages addressed to it
  - Directs messages to specific DPRAM message buffers (predefined service access points serve for addressing buffer #)

AREVA

Message Transfer

- Logical point-to-point connections
  - Separate logical MicroNET communication channel for each message (point-to-point)
  - Designed fixed size of each message
  - Unique MicroNET communication interface independent of type of buses
- Strictly cyclic message transfer
  - Designed single communication cycle time T_{com} for the system (For Oconee: 25 msec)
- Standard message frame
  - Standard header (sender ID, receiver ID, message type, size, cycle count, CRC checksum, ...)
  - Designed fixed size data section
    - Message size determined individually for each message by SPACE code generator

Unified RTE Message Header

Message Framing

TELEPERM XS™ Communication Method

Data Message Transfer via L2 Bus

AREVA

Input Checks of Messages
RTE cycle phase 2

- The integrity of all messages received from other processing modules is checked in phase 2 of the RTE cycle by:
  - Message length and CRC checksum for the occurrence of individual bit errors
  - Message ID, type, sender CPU ID, and receiver (i.e., own) CPU ID to ensure the message is the expected one
  - Sequence number increment to ensure that a new message has been received (message age monitoring)
  - Message status to make sure the message was marked valid by the sender (i.e., sender CPU not in diagnosis mode)

AREVA

Message Age Monitoring

> *Message age monitoring performed by RTE of receiving CPU*
> *Status is based on cycle count of sending CPU*
- NEW
  - New message received and message age check passed
- ONE_MISS
  - Single miss of message and previous message is used again
- INVALID:
  - No valid message available and message buffer marked invalid

Handling of Communication Errors
Message Age Monitoring

> Error situation: A data message cannot be received by the Runtime Environment (RTE) for two (or more) cycles

> Signaling:

- Fault indication at the application software level (binary signal via TXS function block RTE-Output)
- Error message by the RTE sent to the service unit

> Handling of the message buffer:

- Message marked invalid, subsequently …
- … *ERROR* status flag set for all application data contained in the message
  - In this way TXS function blocks used in the application software (FDG module) are able to identify and consider such data as faulty and exclude them from further processing by the application software

TELEPERM XS™ Interchannel Communication

Sean Kelley

Interference-free Communication

> **Use of fiber optic transmission medium**
- Effects caused by electromagnetic interference cannot propagate

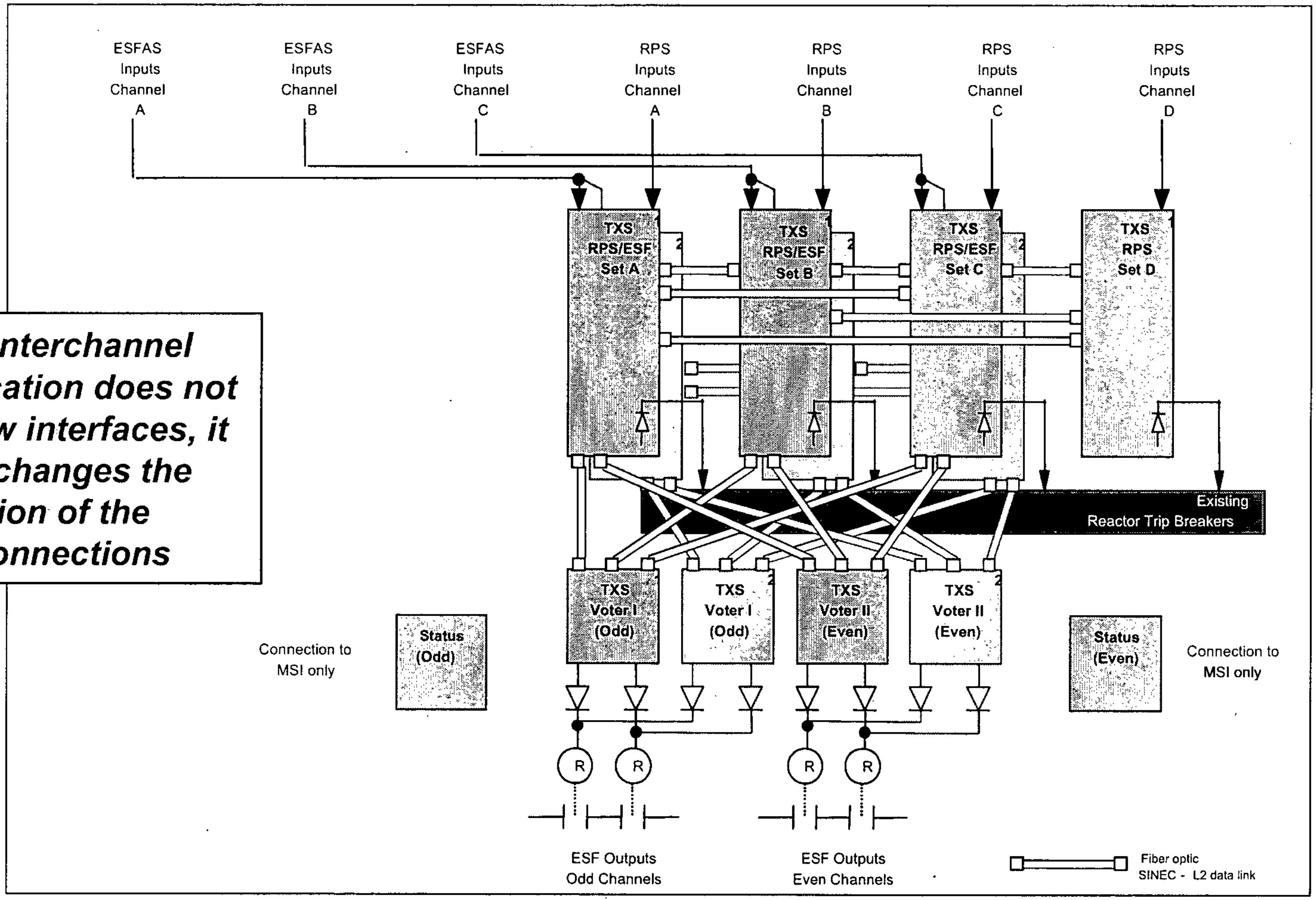
> **Individual DPRAM buffers for each message**
- Separation of the data flow for sending and receiving

> **Cyclic processing of application and communication functions, including message transmission, without any possibilities of influencing linked communication systems**
- Independent control flow of communication module and processing module

> **Check on the received messages to determine whether the transmission has been performed with valid message data**
- Message header and CRC checksum checks along with message age monitoring

> **On-line validation of input data is applied in TXS application software**
- Limits propagation of faulty data
- Provides valid input data for subsequent function diagram module processing

Interchannel Communication Architecture



Use of interchannel communication does not create new interfaces, it simply changes the location of the interconnections

Oconee PPS Interchannel Communication Architecture

Advantages of Interchannel Communications

> Comparison of like process parameters between different safety channels allows:
- Exclusion of faulty signals from trip logic (on-line validation)
- Automatic channel checks for analog signals, asynchronous detection for binary signals
- Reduction of spurious actuation
- Increased system availability (fault tolerance)

On-line Signal Validation

> On-line validation of redundant input data is performed using the 2nd min / 2nd max analog signal selection feature
  - For trip functions looking for decreasing values, the 2nd min logic passes the second lowest value to comparator logic
  - For trip functions looking for increasing values, the 2nd max logic passes the second highest value to the comparator logic

> Similar functionality using 2/4 and 2/3 function blocks for binary signals

> Alarm indication is initiated by these function blocks in order to signal early information about discrepancies between redundant input signals or failure in the I&C equipment

> If one or more of the redundant input data is marked with the *ERROR* status flag, it is excluded using error propagation barriers (i.e. 2.MIN, 2.MAX, 2/4, 2/3, etc. function blocks)

> On-line signal validation functions behave identically and independently of the origin of the detected invalid data and the remaining valid data

On-line Signal Status Processing

Error Propagation Barriers

On-line Analog Signal Processing

No Fault Example

On-line Analog Signal Processing

Failure Example

Spurious Actuation Prevention

> As compared to conventional analog designs, which would actuate one channel on any signal lower/higher than the comparator setpoint, the 2nd min / 2nd max logic compares redundant process data from all channels prior to the setpoint comparison.

> The result is that the process measurement nearest the trip setpoint will not result in an overly conservative spurious trip in any channel.

   - Failed signals do not result in partial trip condition

> Instead, all channels will trip correctly based on the remaining valid 2nd min/ 2nd max inputs.

Increased System Availability

- In conventional analog designs, a channel could fail to trip during a detected 2 out of 3 condition due to a hardware failure in the actuation path of the channel (for example Channel A trip relay)
- With 2nd min / 2nd max logic all channels use all available data in the setpoint comparison thereby ensuring that the overall function is performed correctly

[ ]

TXS Fault Accommodation:
Functional Logic

AREVA

Automated Channel Check Logic

> Currently channel checks are performed manually by operators every 12 hours by reading the individual signals and making a comparison

> 2.MIN and 2.MAX functionality can be used to automatically perform channel checks and alarm any process data that deviates from the other signals by a defined tolerance

> Data that deviates from the other inputs by more than the tolerance amount is alarmed but not excluded from the logic

Interchannel Communication

Summary

> In the PPS, like RPS/ESFAS input parameters undergo integrity and validity checks to determine whether the data is good prior to use
  - This prevents faulty data from being propagated throughout the channel

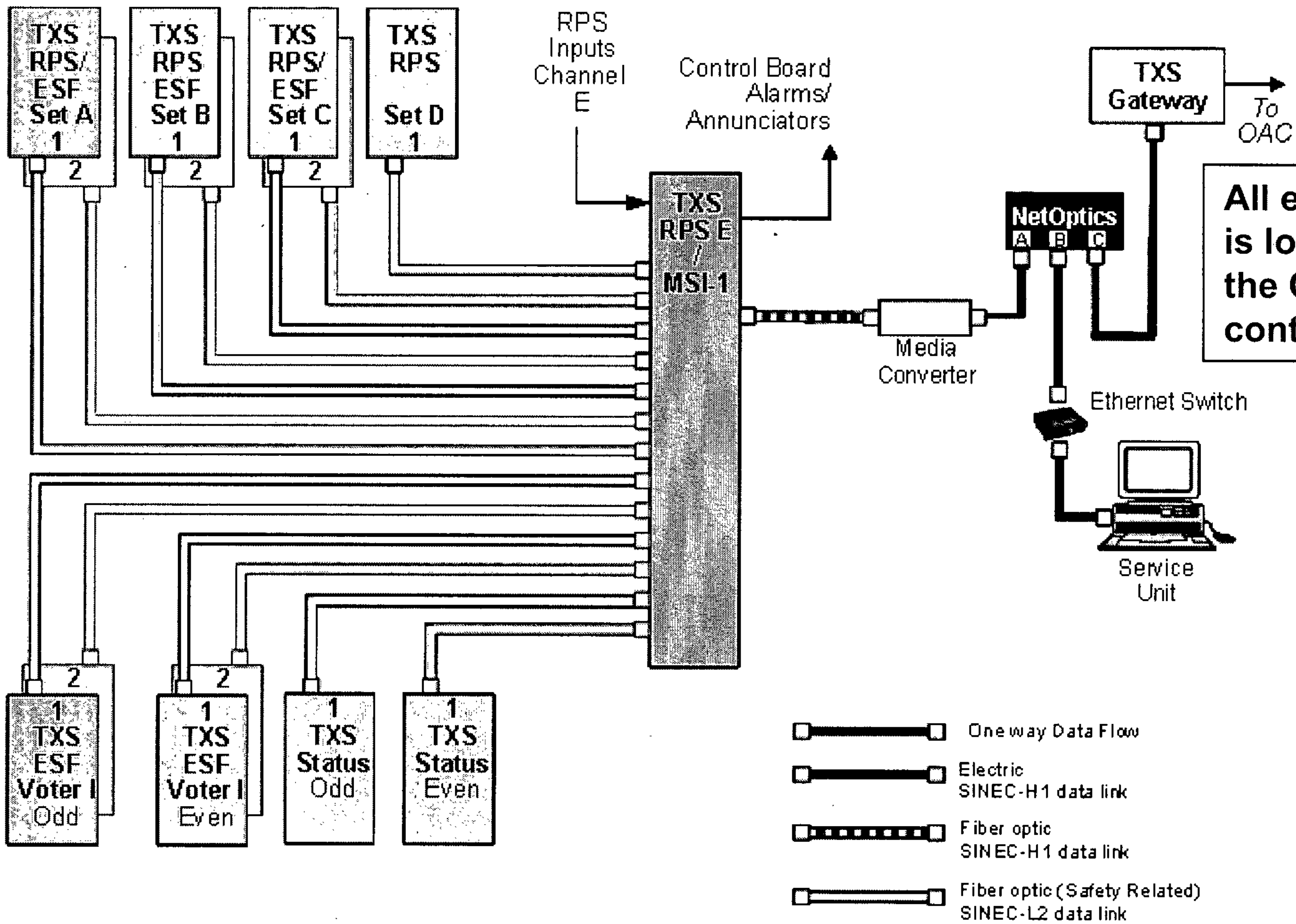
> Faulted data is removed from the measurement, thereby preventing spurious actuation and increasing system availability
  - NOTE: Data that deviates from the other inputs by more than a conservative amount is alarmed but not excluded from the logic

> Alarms are provided for both faulted and deviated data so operator action can be taken to investigate and correct the problem

TELEPERM XS™
Communication with Service Unit

Dr. Steffen Richter

Oconee PPS Architecture



All equipment is located in the Oconee control room

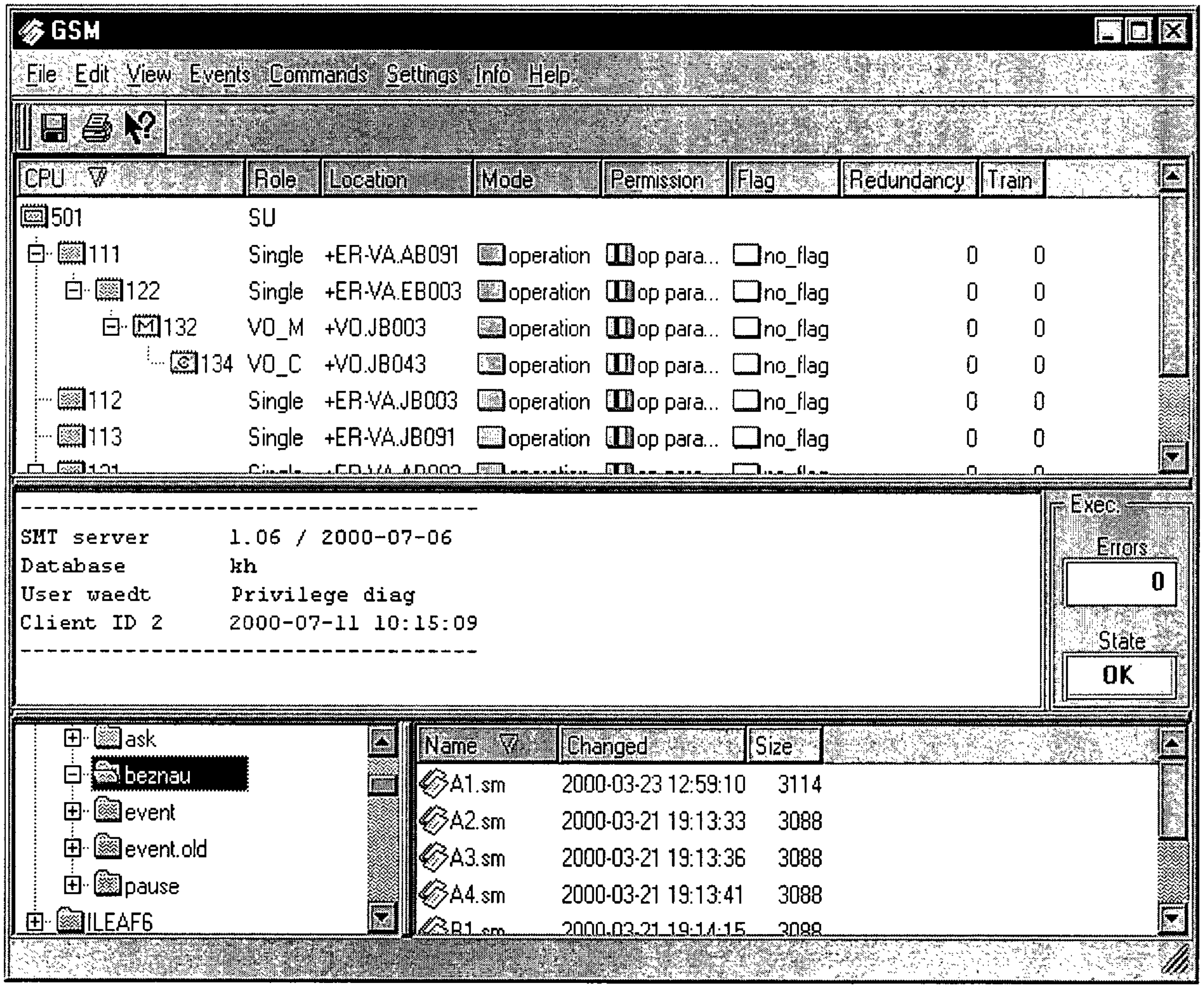
Network Architecture of the New Oconee PPS

Role of MSI Computer

MSI as a Data Transmission Barrier

TELEPERM XS™ Service Unit
Graphic Service Monitor

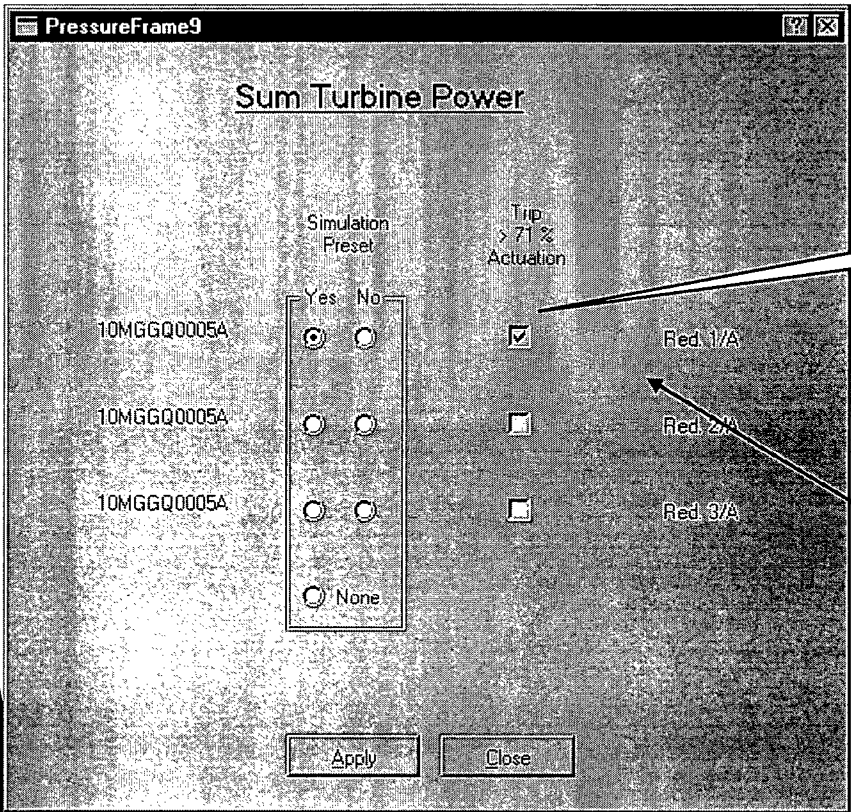
> Overview on CPUs of the TXS I&C system
  - Operating mode
  - Signalization, alarms
> Selection/Execution of pre-defined service actions
  - Parametrization etc.
> Menu-guided service actions
  - Acknowledging
  - Tracing signals
  - Performing tests



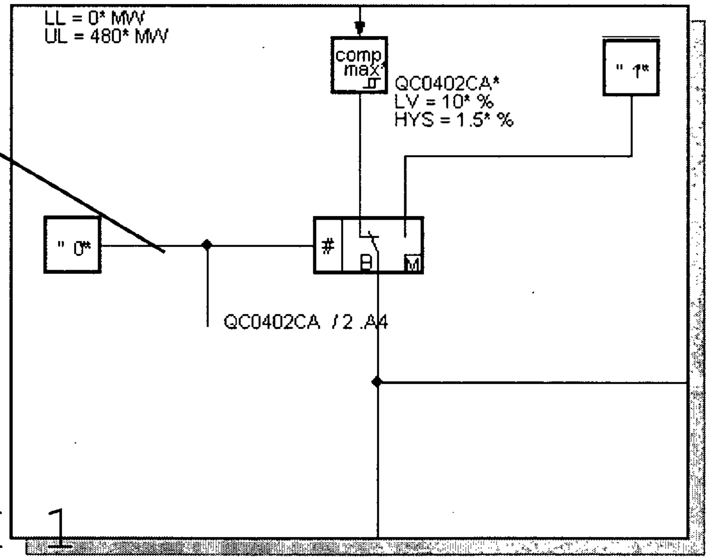
TELEPERM XS™ Service Unit
Dynamic Logic Viewer Function

Graphic Service Monitor

Custom Add-ons: Association to Binary FB Parameter



Switch setting
(binary parameter)



fdVar = FD_1_FB_1_PARAM_1

Access Control

Example: Setting I&C Parameters On-line

Release Conditions

Release Conditions

TELEPERM XS™ Communication
Types of Messages

Message Transfers

AREVA

Signaling Message
Purpose and Content

> Assembled by RTE of each CPU
> In phase 6 of every cycle

> Consists of:
- Signaling message header
- Status indication of the RTE (operation mode, status of release signals, flags indicating fault situations)
- Response to a service command handled before by the RTE (if some)
- Any pending system error messages
- Any requested trace data

AREVA

RTE Service Commands

RTE Operation Modes

Input Check of RTE Service Commands

Communication with Service Unit

Coordination of Tasks in a TXS CPU

Task Activities in TELEPERM XS^{TM} CPU

RTE Service Commands

AREVA

RTE Service Commands (cont.)

RTE Service Commands (cont.)

AREVA

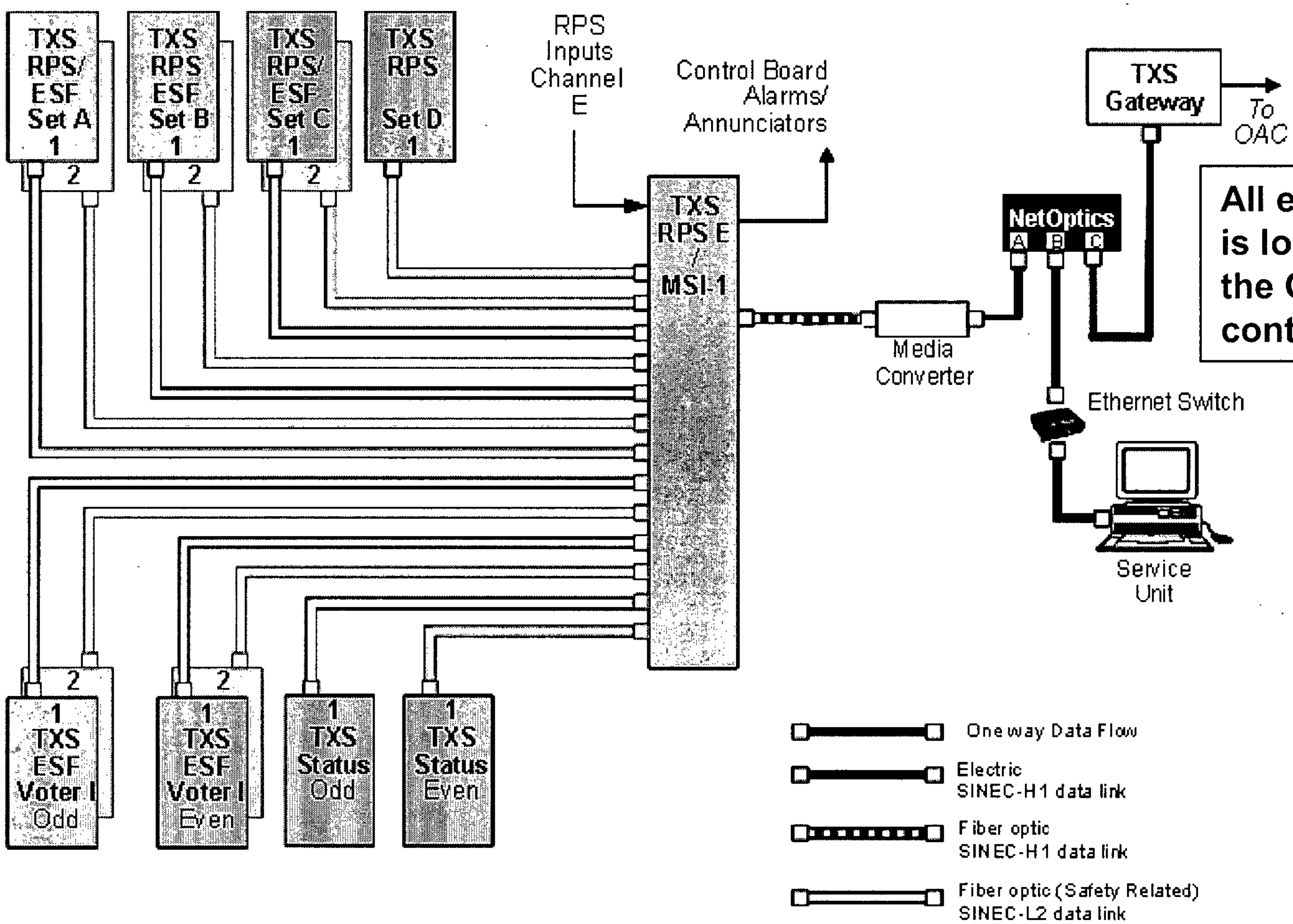
Communication with Service Unit

- Safety to Non-Safety Interface with Service Unit via MSI
- Physical Separation
- Electrical Isolation
- Access Controls for Location of TXS Equipment

TELEPERM XS™
Communication via Gateway

Dr. Steffen Richter

Oconee PPS Architecture



All equipment is located in the Oconee control room

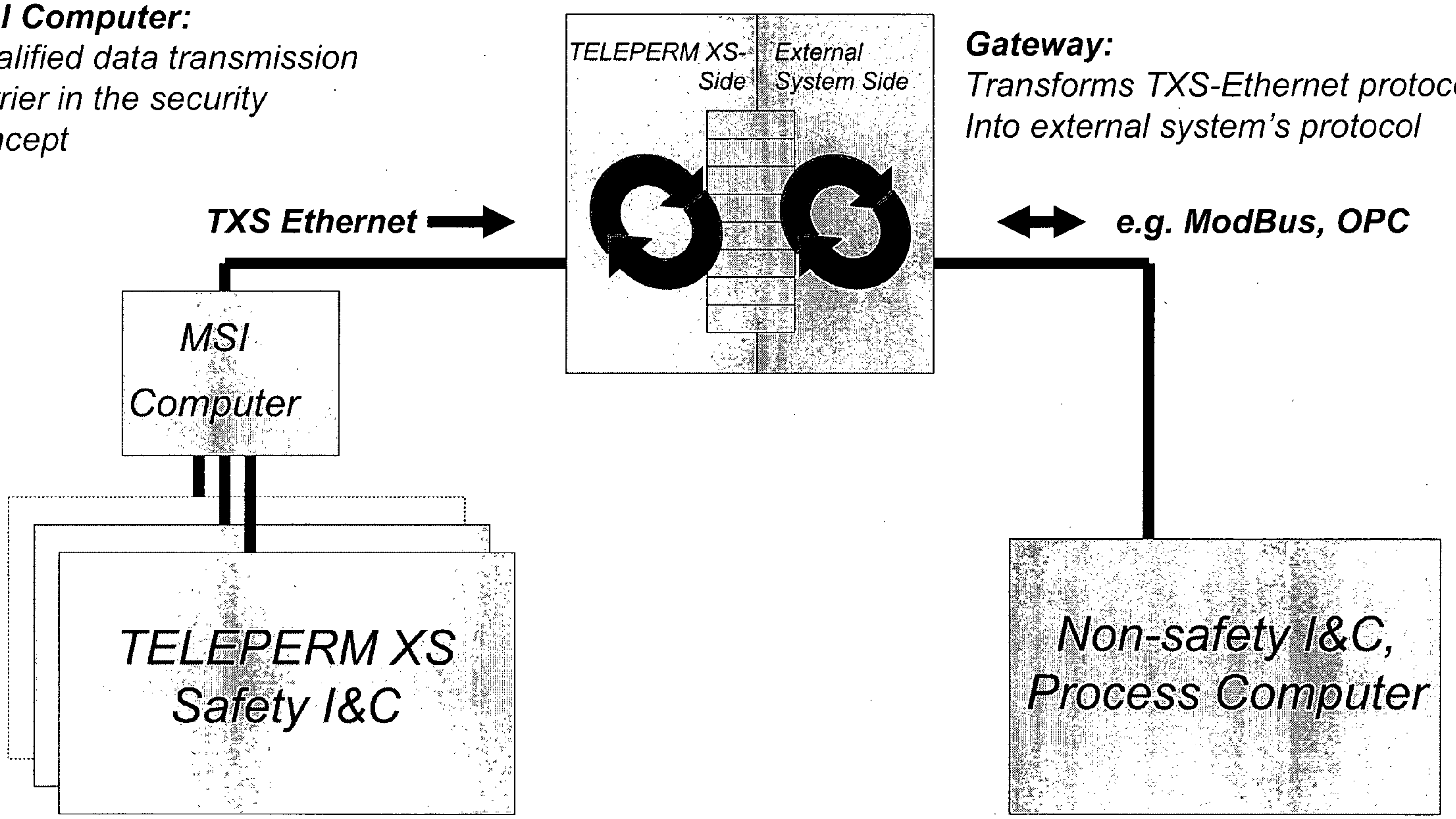
Network Architecture of the New Oconee PPS

TELEPERM XS^{TM} Gateway

External Communication via TELEPERM XS Gateway

MSI Computer:
Qualified data transmission barrier in the security concept

Gateway:
Transforms TXS-Ethernet protocol Into external system's protocol



Regulatory Evaluation

Robert Gill

AREVA

Applicable Regulations and Regulatory Guidance

> Regulations
  - 10 CFR 50.55a(h), Protection and Safety Systems
  - Requires compliance with IEEE 603-1991, Criteria for Safety Systems for Nuclear Power Generating Stations

> Regulatory Guidance
  - Regulatory Guide 1.152, Criteria for Use of Computers in Safety Systems of Nuclear Power Plants
  - RG 1.152 endorses IEEE 7-4.3.2-2003, *Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating* Stations
  - Standard Review Plan
    - SRP Appendix 7.0-A, Review Process for Digital Instrumentation and Control Systems
    - SRP Appendix 7.1-C, Guidance for Evaluation of Conformance to IEEE 603
    - SRP Section 7.9, Data Communication Systems, in NUREG-0800

Interchannel Communication Compliance

- TELEPERM XS system meets IEEE 603 and IEEE 384 requirements for physical, electrical, and communication independence
  - Equipment in different cabinets
  - Fiber optics and qualified optical isolators
  - DPRAM buffering circuits
- TELEPERM XS design features ensure data communication between safety channels does not inhibit the performance of the safety function as required by IEEE 7-4.3.2 and conforms to associated regulatory guidance (i.e., RG 1.152, SRP 7.1, SRP 7.1-C and SRP 7.9)
  - Strictly cyclic processing of application software
  - Asynchronous operating system
  - Static memory allocation
  - Message transfer controls
  - Absence of process-driven interrupts
  - Constant load on bus systems
- TELEPERM XS signal validation techniques improve system performance and meets IEEE 603 and IEEE 379 requirements
  - Error propagation barriers
  - Not vulnerable to single failures
  - Additional fault detection and accommodation capabilities

Communication with Service Unit Compliance

- TELEPERM XS system meets IEEE 603 and IEEE 384 requirements for physical, electrical, and communication isolation
  - Fiber optics and qualified optical isolators
  - DPRAM buffering circuits
- TELEPERM XS design features ensure data communication between safety channels does not inhibit the performance of the safety function as required by IEEE 7-4.3.2 and conforms to associated regulatory guidance (i.e., RG 1.152, SRP 7.1, SRP 7.1-C and SRP 7.9)
  - Strictly cyclic processing of application software
  - Asynchronous operating system
  - Static memory allocation
  - Message transfer controls
  - Absence of process-driven interrupts
  - Constant load on bus systems
- Oconee design provides multiple layers of access control to prevent unauthorized access to or use of the MSI as required by IEEE 603, IEEE 7-4.3.2 and conforms to associated regulatory guidance (i.e., RG 1.152, SRP 7.1, SRP 7.1-C and SRP 7.9)
  - All equipment located in control room
  - Controlled access location within control room for service unit
  - Key lock controls
  - Password/privilege controls

Communication with Gateway Compliance

- Oconee design provides one-way communication to the Gateway as required by IEEE 603, IEEE 7-4.3.2 and conforms to associated regulatory guidance (i.e., RG 1.152, SRP 7.1, SRP 7.1-C and SRP 7.9)

AREVA

Acronyms

> **CPU:** Central Processing Unit
> **CRC:** Cyclic Redundancy Check
> **DCS:** Data Communication System
> **DPRAM:** Dual Port Random Access Memory
> **EPROM:** Erasable Programmable Read Only Memory
> **EEPROM:** Electrically Erasable Programmable Read-Only Memory
> **ESF:** Engineered Safety Feature
> **ESFAS:** Engineered Safety Feature Actuation System
> **FB:** Function Block
> **FDG:** Function Diagram Group
> **HW:** Hardware
> **I/O:** Input/Output
> **ID:** Identification

Acronyms

- **MSI:** Monitoring & Service Interface
- **OAC:** Operator Aid Computer
- **PPS:** Plant Protection System
- **RAM:** Random Access Memory
- **RPS:** Reactor Protection System
- **RTE:** Runtime Environment
- **SER:** Safety Evaluation Report
- **SPACE:** Specification and Coding Environment
- **SRP:** Standard Review Plan
- **TCP/IP:** Transmission Control Protocol/Internet Protocol
- **TXS:** TELEPERM XS™