Safety and Nonsafety Communications and Interactions in International Nuclear Power Plants

Roger Kisner

R. Kisner, J. Mullens, T. Wilson, R. Wood, K. Korsah, A. Qualls, M. Muhlheim, D. Holcomb, and A Loebl

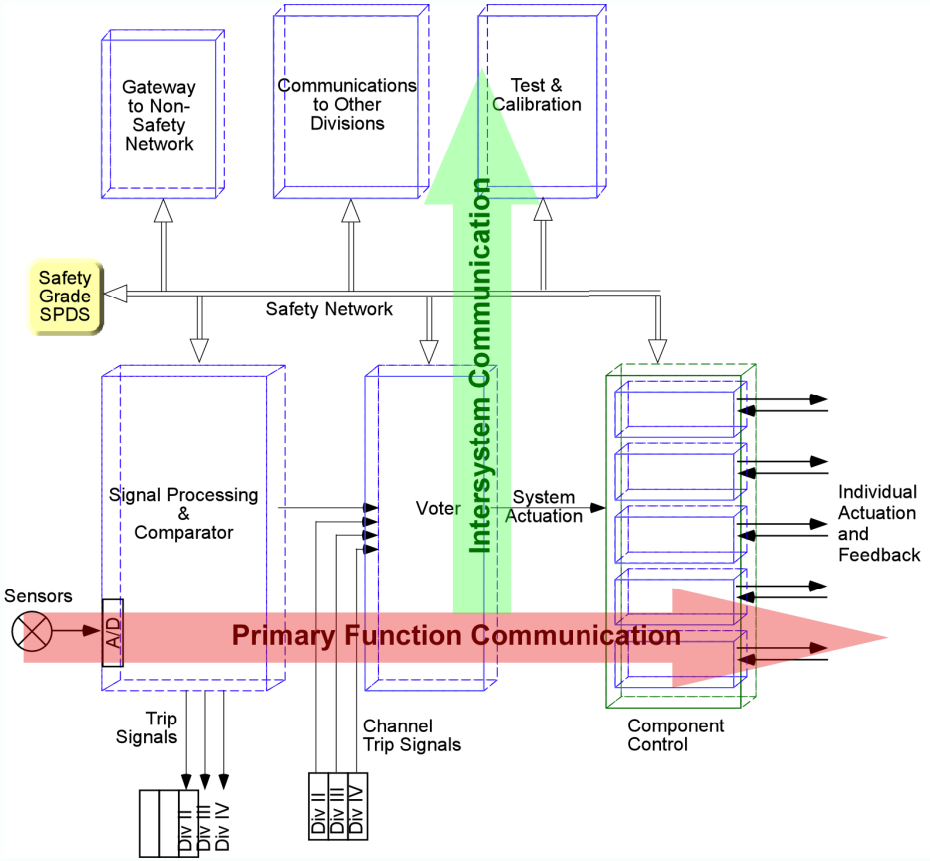
NRC Project Manager: Paul Rebstock

Presentation to NRC Technical Working Group on Highly Integrated Control Room Communications
June 14, 2007

OAK RIDGE National Laboratory

Basic Intent of the Report: Investigate Safety System Intercommunication

- Communications types and structures used in a representative set of international nuclear power reactors
- Communications issues derived from standards and other source documents relevant to safety and nonsafety communications



Topics Discussed in the Report Target Digital Communication

- Communication among redundant safety divisions
- Communications between safety divisions and nonsafety systems
- Control of safety equipment from a nonsafety workstation
- Connection of nonsafety programming, maintenance, and test equipment to redundant safety divisions during operation

Guidelines for Report Preparation

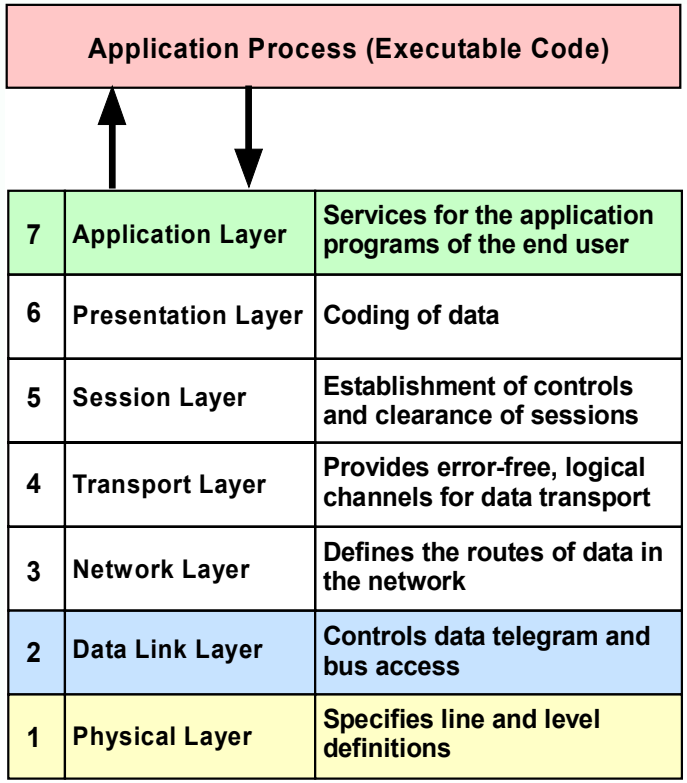
- All material is public domain — no proprietary information
- Concurrence by respective international reactor representatives
- Nine researcher team made contributions to technical survey and best practice review

Report Is Organized around Investigating International Reactors and Existing Standards

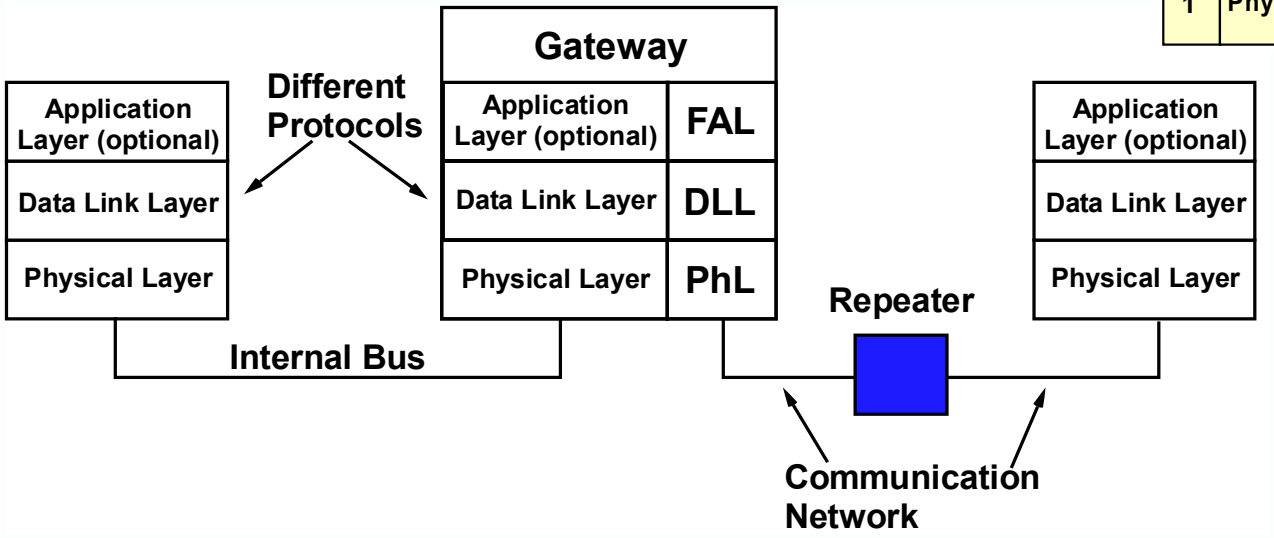
- Introduction
- Communication Vulnerabilities
- International Nuclear Station Review
- Consensus Practices
- Conclusions
- Appendices
- References

A Context Is Built for Network Architectures

- Seven layer OSI model
- Network topologies
- Three layer model for safety systems



7	Application Layer	Services for the application programs of the end user
6	Presentation Layer	Coding of data
5	Session Layer	Establishment of controls and clearance of sessions
4	Transport Layer	Provides error-free, logical channels for data transport
3	Network Layer	Defines the routes of data in the network
2	Data Link Layer	Controls data telegram and bus access
1	Physical Layer	Specifies line and level definitions



Error Types Related to Source, Transmission Channel, Receiver, and System Are Addressed

Communications

- Corruption
- Unintended Repetition
- Incorrect Sequence
- Loss
- Unacceptable Delay
- Insertion
- Masquerade
- Addressing

Sender/Receiver

- Buffer Overflow
- Data Out of Range
- Incorrect Ordering
- Very long delays in bridges and routers
- Very long times to initiate communications

Message Types Relevant to Safety Applications Are Discussed

- Comparison of communication error types with OSI layers
- Message types and error effects
  - Software Coding (Programming Updates)
  - Set-Points and Parameters
  - Command Functions
  - Go/No-Go (Interlocks)
  - Data Streaming
  - System Status

Goal of International Reactor Survey was to Investigate Communication Approaches

- Communication interconnects between safety and non-safety systems and among redundancies
- Technology employed
- Strategies to ensure independence (e.g., no interlinks between functionally diverse subsystems)
- Fault management approaches to preclude communication-based failure or limit the severity of failures
  - Interlocks
  - Detection and correction
  - Message validation

Review of Seven Plants Cuts Across Several NSS Types in Six Countries

- Chooz B PWR (France)
- Sizewell B Westinghouse PWR (United Kingdom)
- Darlington CANDU (Canada)
- Lungman ABWR (Taiwan) Not Yet Operational
  - Unit 1 scheduled for 7/09
  - unit 2 scheduled for 7/10
- Temelin VVER (Czech Republic)
- Dukovany VVER (Czech Republic)
- Olkiluoto-3 EPR (Finland) Under Construction

Chooz B

- Communication exists from lower-grade safety-class systems to Class 1E systems
  - all such communications are point-to-point
  - 4-20 mA current loops or voltage input are used
  - most communicate binary values representing on/off states of a piece of equipment
- Communication from control room down to actuators for non-safety automatic, or manual control inputs, to the non-safety actuators, travel through the Level 2 plant network to the Level 1 automation system (Contronic E)
- Signals that actuate dual-use, safety and non-safety components pass down to the priority module (for arbitration) before actuation of the safety device
- The protection system (SPIN N4) contains internal network interconnections using dedicated Ethernet-based protocol
  - Trip/no trip calculations are performed on sensors associated with a division and the results are compared among the four divisions
  - No inter-division validation of the measurements is performed
- Nearly all Class 1E functions are completely automatic
  - The few manual operations are hard-wired – no soft controls provided

Sizewell B

- Primary protection system is digital (W Eagle 2000) while secondary protection system is hardwired (Laddic)
- High speed data links between microprocessors (MP's) performing detection, voting, and actuation functions
  - Optical fiber for isolation between divisions
  - Defined data format, fixed length, message validation
- Proprietary network (Westnet) interfaces via gateways with the primary safety system for auxiliary functions
- Automated self-testing computer for each division communicates via a dedicated network connection

Darlington

- Darlington employs a graded safety classification system
- All components of the shut down systems must meet qualification standards
- Communication from less rigorous safety classes to the more rigorous safety classes is over separate optical fiber links that must be enabled using mechanically activated interlocks
- Interlocks prevent concurrent external communication to more than one safety division within a shut down system

Lungman

- RPS communicates to the plant data network and triple modular redundant control systems using RS-485 protocol over optical fiber to one-way protocol interchange gateways
- ESF network rings also communicate to the non-safety plant networks via one-way, buffered protocol interchange gateways
- All commands to safety systems are communicated only over safety-grade channels from safety-grade controls

Temelin

- **Similar to Sizewell, except**
  - **Manual controls are part of safety system**
  - **Triple redundant divisions (2oo3 voting) instead of quad**
  - **Upgraded plant network to FDDI**
  - **CPU's upgraded to Intel 80486**
  - **Mobile tester for testing one channel at a time**

Dukovany

- Protection system is SPINLINE 3
- Communications for all protection and auxiliary functions is on custom NERVIA network
  - SPINLINE product
  - 10 megabit/sec
  - Deterministic, broadcast-type, token ring
  - Message testing (checksum)
- One network per division
- Loss of any component, network or microprocessor, does not cause another component to stall
- All NERVIA networks connect through gateway to plant information Ethernet network

Olkiluoto-3

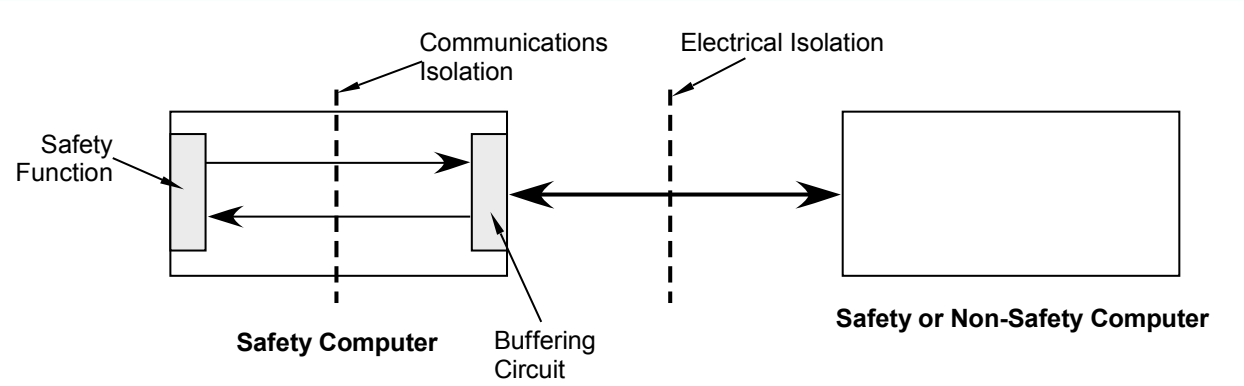
- **Monitoring and Service Interface (MSI) provides the communication link between the safety system (all four divisions) and other systems**
  - **MSI is within the boundary of safety grade systems based on a graded classification approach**
  - **MSI provides the interface to the safety panels and plant computer via a gateway**
- **Limited two-way communication through the MSI can be enabled for maintenance and testing of the safety system**
  - **Communications through the MSI are validated to allow only pre-defined messages to be transferred to the safety system**
  - **Communication from the maintenance service unit to a safety division can only be enabled via a key switch**
  - **Interlocks prevent concurrent communication to more than one safety division**

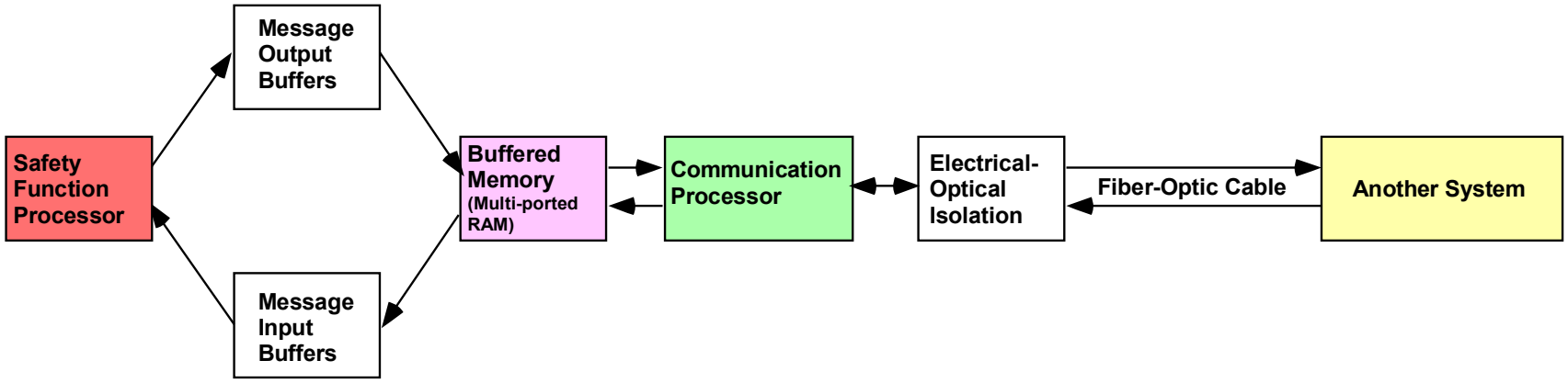
Report Examines Key Standards Relevant to Digital Communications

- **IEEE 603-1998; IEEE 7-4.3.2-2003**
- **IEC 61500 (2002)** ***Nuclear Power Plants—Instrumentation and Control Systems Important to Safety—Functional Requirements for Multiplexed Data Transmission***
  - **15 major recommendations**
- **IEC 61508 (working draft 2005)** ***Functional safety of electrical/electronic/programmable electronic safety-related systems—Part 1***
- **IEC 61513 (2001)** ***Nuclear power plants—Instrumentation and control for systems important to safety—General requirements for systems***
- **IEC 61784-1 (2001)** ***Digital data communications for measurement and control—Part 1: profile sets for continuous and discrete manufacturing relative to Fieldbus use in industrial control systems***
- **IEC 61784-3 (2006)** ***Digital data communications for measurement and control—Part 3: profiles for functional safety communications in industrial networks***

Logical and Electrical Buffering for Independence of Safety from Other Safety or Non-Safety Systems

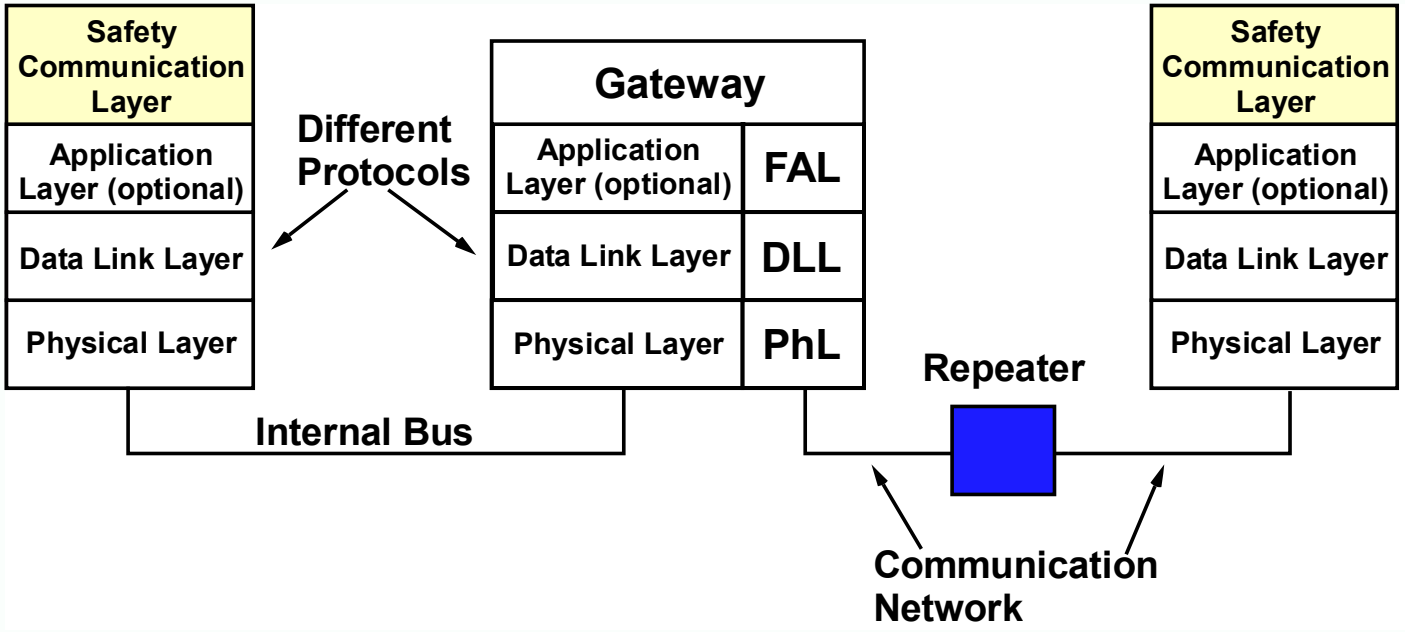
IEEE 7-4.3.2 Annex E





Safety Communication Layer Described in IEC 61784 as OSI-Based Method to Maintain Safety Regardless of Communication Errors

- Detect and handle safety-related communication errors
- Safety communications error responses
  - Correct (recover)
  - Take safety action (go to safe state)
- Must act within required safety response time
- Reliability according to design SIL (1 – 4)

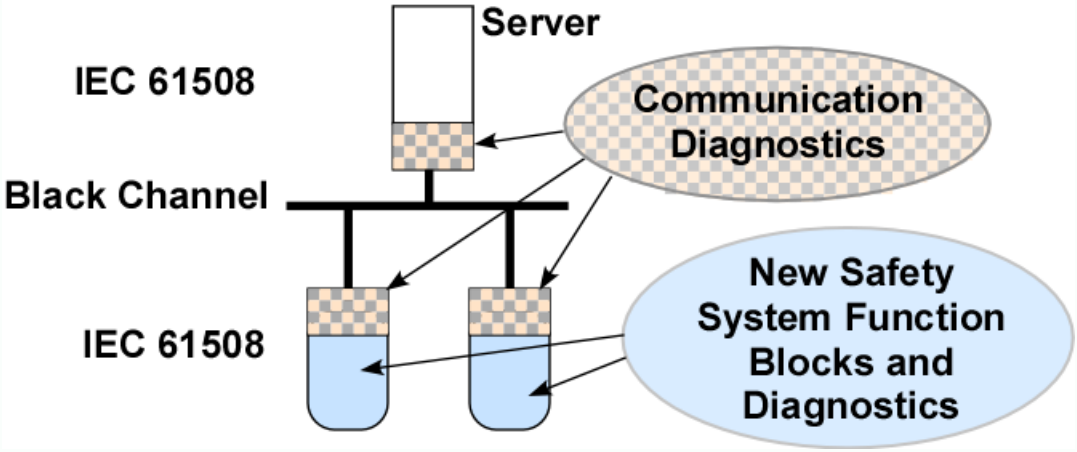


Possible Communication Errors and Protection Measures

Comm. Errors	Safety Measures							
	Seq. Number	Time Stamp	Time Exp.	Connection Authent.	Feedbk Mess.	Data Integrity Assur.	Redund. with Cross Checking	Diff. Data Integrity Assur. Sys.
Corruption					X	X	Only for Serial bus	
Unintended Repetition	X	X					X	
Incorrect Sequence	X	X					X	
Loss	X				X		X	
Unacceptable Delay		X	X					
Insertion	X			X	X		X	
Masquerade				X	X			X
Addressing				X				

Black Channel

- "Black channel" comes from the idea that the safety-related message content is unknown to the non-safety communications link
- "White channel" is (entirely) safety grade equipment



- Non-safety communications link carries safety-related messages
- Other equipment on the link might not be safety equipment
- Safety Communications Layer (on each safety-related network node) protects against errors in safety-related messages caused by non-safety equipment

Conclusions Section Summarizes Top Points from Report

- Structured approach for evaluation of communications systems has emerged
  - Safety-to-safety
  - Nonsafety-to-safety
- Two general failure categories
  - Information
  - Communication
- Two failure outcomes
  - Interruption of safety function execution (code execution stops)
  - Incorrect functioning of safety system (incorrect decision)