OAK RIDGE
NATIONAL LABORATORY
MANAGED BY UT-BATTELLE
FOR THE DEPARTMENT OF ENERGY

ORNL/NRC/LTR-07/05

Safety and Nonsafety Communications and Interactions in International Nuclear Power Plants

August 2007

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

NRC Manager: P. Rebstock
ORNL Manager: R. Wood

UT-BATTELLE
ORNL-27 (4-00)

ORNL/NRC/LTR-07/05

Engineering Science and Technology Division

Safety and Nonsafety Communications and Interactions in International Nuclear Power Plants

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

NRC Manager: P. Rebstock
ORNL Manager: R. Wood

Guidelines for the Design of Highly Integrated Control Rooms

August 2007

Prepared for the
U.S. Nuclear Regulatory Commission
under
DOE Interagency Agreement 1886-N640-9W
NRC JCN No. N6350

Prepared by the
OAK RIDGE NATIONAL LABORATORY
Oak Ridge, Tennessee 38731-6285
managed by
UT-BATTELLE, LLC
for the
U.S. DEPARTMENT OF ENERGY
under contract DE-AC05-00OR22725

CONTENTS

Page

LIST OF FIGURES

LIST OF TABLES

1. INTRODUCTION

Oak Ridge National Laboratory (ORNL) is conducting research regarding digital system technical issues associated with highly integrated control rooms (HICRs). In particular, ORNL has investigated digital communications technology and implementation practices to support development of the technical basis for review guidance. As part of this study, ORNL has surveyed information on the use of digital communications at several international nuclear power reactors. The findings of these surveys, along with a summary of particularly relevant communication standards related to safety, are presented.

1.1 BACKGROUND

In an HICR environment, information from numerous control and safety systems is displayed in the main control room. It is possible to integrate information from several systems onto a single display or to have isolated displays for individual systems. For most systems, integration presents little difficulty. Data can be shared by multiple machines and transferred using a data transfer protocol. Screens that display information from control systems rely upon enabling logic to request information. In many implementations, remote terminals operate by issuing a request for data that causes the controlling computer to interrupt its processing sequence to respond to the request. During off-normal events, personnel often populate all available remote displays and request as much information as they deem useful.

Care must be taken so that requests for information do not interfere with the functionality of controllers. A common means of minimizing such interference for control and protection systems is to pass information to display systems using a fixed message structure, using a network in a ring topology, and always passing complete information to each node on the network with deterministic timing, thereby avoiding processing sequence interruption. For nonessential displays, a common methodology to avoid interference with the plant safety network is to connect the displays to a secondary nonsafety network that includes an information server connected to the safety network through a one-way information gateway[*] that provides safety data to the nonsafety network. On a physical layer, fiber-optic connections are used to isolate critical systems galvanically.

A control system must be properly designed and implemented to perform its intended function. Confidence that a system is properly designed is generated through verification and validation. Physically checking connection points, component specifications, and individual functionality are part of the validation process. Functional checks are used to verify that equipment interfaces are properly designed and that the integrated system, including logic and hardware, is implemented to perform as specified in the functional requirements document.

End-to-end functional testing can only verify and validate the performance of a control system for the tested sets of conditions. Unless all possible sets of conditions can be anticipated and tested, the functional testing is inherently limited. It generally is useful in determining whether a component will perform as anticipated under prescribed conditions, but it cannot provide an indication of system functioning under unforeseen circumstances. An example of a digital control system malfunction in a nonpower reactor application is described in Nuclear Regulatory Commission (NRC) Information Notice 93-57. The control system for a Training Research and Isotope production—General Atomics (TRIGA) reactor contained control rod interlock logic. The system also received commands from pushbuttons on a control console. When a trainee simultaneously depressed the reactor pulse mode selection button and the rod withdrawal button, the control system began withdrawing the control rod,

[*]There are some exceptions to this, such as the Olkiluoto-3 (OL-3) and the U.S. EPR. The I&C architectures of these plants employ two-way communication between the Process Information and Control System (PICS) and the Protections System/Safety Automation System (PS/SAS). See Sect. 3.10 for a more detailed description.

which was not allowed with the reactor in pulse-mode, and did not stop when the withdrawal button was released. A manual scram initiated by an operator was required.

For that reactor, it was determined that an error in the logic allowed this to occur and that the error could occur in more than one operating mode. The origin of the logic error was in the functional requirements specification. However, the fault was embedded in the software, but it was not detected during functional testing because the vendor did not test the simultaneous depression of more than one control switch; thus, although the system passed a functional test, it was still flawed. A software modification was required to correct the problem.

Another event (also recorded in NRC Information Notice 93-57) occurred when an operator entered an out-of-range value (in this case, an incorrect sign) for an input variable. Because of lack of input validation and a logic error, the incorrect value caused the control rod to withdraw.

These occurrences illustrate the difficulty in developing a complex monitoring and control system. Logic can be influenced by event sequencing, and incorrect responses can occur because of unanticipated control input. It is not practical to discover all potential modes of malfunction for a complex digital control system. A strategy to increase the probability of proper action is to validate the system within a well-defined operational envelope and limit operation to that envelope. This concept-of-operation requires strict adherence to operating procedures and does not protect against inadvertent deviation from those procedures. One might erroneously believe that strict adherence to operating procedures (that keep the configurations, thresholds, etc. in their design regions) would be completely protective.

1.1.1 Communications

Monitoring of the overall condition of the plant can be performed from a control workstation. Multiple operational functions can be implemented at a single station, such as displaying trends in signal values or the currently measured parameters against their set point values. Modern control networks also allow updating instrumentation calibration constants from maintenance terminals.

Coherent presentation of plant status to the operators requires integration of instrumentation and control (I&C) subsystems that, in turn, requires data sharing from many systems. The method of sharing information across the various subsystems is an important part of system design and configuration. Critical issues include validation of displayed information and control hierarchy for redundant terminals.

Each of the levels within a nuclear power plant's (NPP's) defensive measures is required to be independent and diverse. This includes an independent, diverse reactor trip mechanism. While the diverse reactor shutdown system is required to be of high quality, it is not required to be safety class. Additionally, the overall plant control systems are not required to be safety class. The interaction between the various safety and control subsystems can lead to subtle operational difficulties.

Digital I&C systems typically generate a significant volume of data; the display provides situational awareness to the operators. Network-connected computers allow data recorded by the system to be displayed at various places in different ways for different purposes. General communication and information display guidelines arise from prior communication system problems and the safety and control requirements of NPPs.

1. *Safety-System Interference*—Requests for data must not interrupt the collection of data and must not interfere with the display of data for critical systems.
2. *Data Pedigree*—The pedigree (i.e., the history and validity) of information presented to plant operators must be assured. During the data networking and signal processing, data may be delayed or corrupted.
3. *Reliance on Nonsafety-Grade Information Display for Safety Actions*—Nonsafety-grade terminals allow displaying more detailed plant status information as well as implementing normal plant control instructions. However, nonsafety-grade information displays may become corrupted or

unavailable during plant transients. This can be problematic if the plant operators are accustomed to receiving all (including safety parameters) of the plant status information from the nonsafety-grade displays. Rigorous administrative control is required to ensure that operators are not solely reliant on nonsafety-grade displays for safety-grade information.

4. *Limitation of the Consequences of Operator Errors*—Operators can make incorrect decisions or improperly execute correct decisions. As a result, control architectures can contain systems that monitor operator actions and prevent or limit any that are found to be detrimental to plant safety. Typically, such systems are functionally placed between the control system and the protection system such that challenges to the protection system are reduced.

1.2 PROBLEM STATEMENT

Current industry and NRC guidance documents such as Institute of Electronic and Electrical Engineers (IEEE) 7-4.3.2, Regulatory Guide 1.152, and IEEE 603 do not sufficiently define a level of detail for evaluating interdivisional communications independence. The NRC seeks to establish criteria for safety systems communications that can be uniformly applied in evaluation of a variety of safety system designs. This report focuses strictly on communication issues related to data sent between safety systems and between safety and nonsafety systems. Further, the report does not provide design guidance for communication systems nor present detailed failure modes and effects analysis (FMEA) results for existing designs.

This letter report describes communications between safety and nonsafety systems in NPPs outside the United States. A limited study of international nuclear power plants was conducted to ascertain important communication implementations that might have bearing on systems proposed for licensing in the United States. This report provides that following information:

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

Topics that are discussed include the following:

- communication among redundant safety divisions,
- communications between safety divisions and nonsafety systems,
- control of safety equipment from a nonsafety workstation, and
- connection of nonsafety programming, maintenance, and test equipment to redundant safety divisions during operation.

Information for this report was obtained through publicly available sources such as published papers and presentations. No proprietary information is represented.

1.3 REPORT ORGANIZATION

Many chapters can be written on theoretical and practical aspects of network design and signal processing; however, this report focuses on only a few important topics relevant to safety-related communication. The report is divided into three major sections: communication vulnerabilities, international nuclear plant experience (approaches), and consensus practices. Background information on communication abstraction layers, network topologies, and message and error types as they apply to nuclear safety applications are described in the section, “Communication Vulnerabilities.” The next section, “International Nuclear Plant Experience,” describes digital communications at six different international nuclear power reactors. This section also provides further discussion on communication networking as derived from a review of these reactors. The next section, “Consensus Practices,”

reviews several U.S. and international standards. The ensuing discussions extract communication-related information such as guidelines and best practices that are relevant to licensing nuclear plants in the United States. The “Conclusion” describes a simplified evaluation process derived from information in the preceding sections. Appendixes provide a table on the seven-layer communication abstraction model and lists several communication-related criteria from the *Code of Federal Regulations*.

2. COMMUNICATION VULNERABILITIES

Communications networks that connect safety-grade systems to other safety-grade systems will likely be considered safety-grade themselves. In contrast, network devices that are designed to be credited as physical and logical isolators are used to connect safety systems to nonsafety systems. The portions of the network designed for safety use and the isolator are designed to safety criteria. The nonsafety portion of the communication network does not have to be designed to safety criteria, other than to ensure that faults and failures cannot propagate back into the safety portion of the network. In either case, the application of IEEE 603 requires that the safety system be designed to continue its safety function in the presence of a single failure (see also 10 CFR Part 50, Appendix A, Criterion 21). Therefore, safety systems must be designed to perform their designated protection function in the presence of faults and failures in the nonsafety communication pathways connected to the safety systems.

This section provides background information on the fundamentals of communications and communication vulnerabilities as they relate to nuclear safety applications. The primary issue of digital data communication to a safety system can be summed up in two failure scenarios: (1) loss of communication,* which is a failure to communicate any necessary data when it is needed, and (2) creation of erroneous information. For either scenario, data (or the lack thereof) from any source should not inhibit a receiving safety system from performing its designated function.

2.1 COMMUNICATION NETWORK ARCHITECTURE CONTEXT

2.1.1 Communication Networking Abstractions

The Open Systems Interconnection (OSI) model for network communications identifies seven layers that function to convey data from source to receiver. The model defines a networking framework for implementing protocols in seven layers. Protocols enable an entity in one host to interact with a corresponding entity at the same layer in a remote host.† The layers are shown in Fig. 2.1. Appendix A contains further description of the layers.

The message passing between layers progresses something like this: a message is passed on the source side from layer seven down to layer one to transmit a message from one application to another. Each layer, if present, appends its layer-specific control data as well as a protocol header. These appended data are used to communicate with the corresponding layer on the recipient side. A large amount of control data is transmitted over the physical medium to the receiver in addition

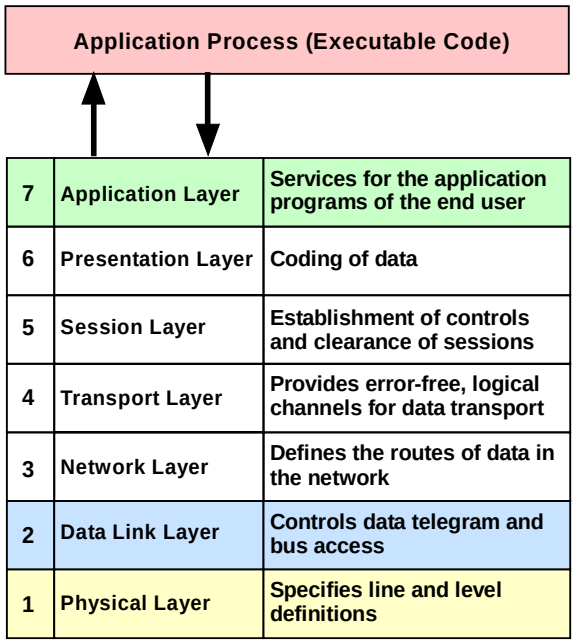

Fig. 2.1. OSI model layers and their relation to executable code.

*A loss of communication can be partial or intermittent. Data sufficiently delayed can be considered either lost or corrupted information.

†OSI protocol work subsequent to the publication of the original architectural standards has largely ceased. The pure seven-layer model is more historic than current but makes an excellent model for discussing the layered protocol approach. Not every modern protocol fits into one of the seven basic layers. Not every protocol provides or needs all seven layers.

to the original message. At the receiver, the message is passed from the physical layer up to the application layer, while each layer performs its requested service and removes its specific control data. The application layer makes the message available to the application process in its original form.

A network is formed wherever nodes are connected. The network node link can be extremely simple. For example, a dedicated point-to-point connection between two nodes such as a serial link with separate transmit- and receive-lines has trivial implementations of the OSI network layers (see Appendix A). However, for whatever reasons the nodes were interconnected, the nodes interact, and their behavior depends on that connection; communications issues such as maximum message delay time become part of the design.

Network links can be point-to-point (i.e., two nodes) or bus media (i.e., more than two nodes). Point-to-point links, which can be designed to operate very simply, are the preferred link for communications related to safety systems interconnection. Point-to-point networking, which has more limited types of failures modes because there are fewer nodes, is the most prevalent and is more straightforward to analyze. The bus has more complicated operation and more opportunities for common cause failures due to its interconnections with issues of media access contention, node addressing, and traffic congestion in addition to failure modes, fault propagation, and common cause failures due to the shared bus. Busses have contention and congestion problems when nodes act independently to gain access and transmit messages. Token passing busses are highly visible shared busses that are engineered to approximate the inherent characteristics of a point-to-point network and reduce media access contention and congestion (at least for most messaging protocols). They do, however, trade-off response time (messages cannot be sent as soon as they are created, but must wait for the token); point to point can run full time. New failure modes of (1) dropped token and (2) duplicate token are introduced with token passing networks. The bus media's complexity requires a more complex design and testing effort. Note that rings and busses can be designed to be deterministic.

New NPPs (Generation III+) extensively depend on networked communications to transmit data within and among various control and safety systems. The network can be configured as any one of several topologies—the result being successful transmission of data from source to one or more receiver.

Network topology refers to the graph properties of the connections among network nodes, independent of the medium, transmission speed, and other properties. A network has three types of topology:

1. physical topology—the physical connections among the nodes,
2. signal topology—paths taken by the physical network signals among the nodes, and
3. logical topology—the flow of information between the nodes.

For example, a network might consist of all nodes on a local area network (LAN) being *physically* tied to a central switch that also connects to a wide area network (WAN). The switch might route *signals* only to the destination nodes or might route all signals to all nodes, and the network protocol could require a token ring style of *logical* behavior in which data are passed sequentially among the nodes. All three types of topologies influence the network's failure modes, fault propagation, and fault handling properties. Typical (nonredundant) network topologies are shown in Fig. 2.2.

2.1.2 Safety Networks

Safety-critical networks are designed for high reliability. Features such as flexibility, handling multiple protocols, and wide area coverage with many nodes are not needed for safety critical systems and are not recommended because these features may lower communications reliability and introduce unpredictable delays in sending messages between nodes.

In a fully developed bus network structure, all seven layers may be functioning to accomplish the routing and the compatibility needed over a general high-speed network; however, for point-to-point

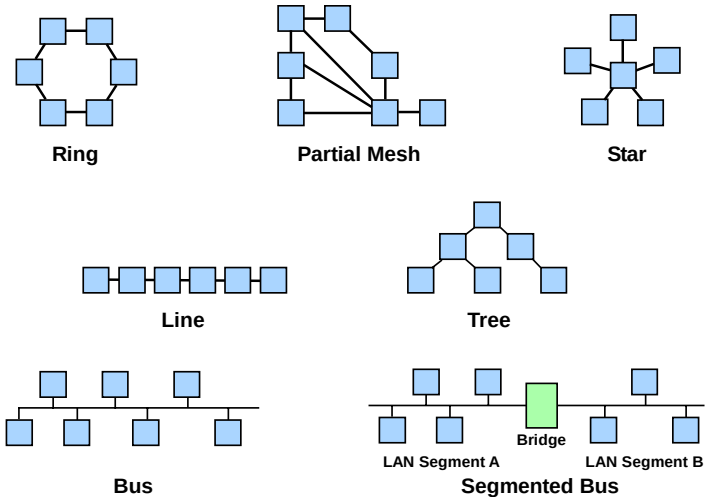

Fig. 2.2. Typical communications network topologies.

and otherwise constrained instrumentation networks typically used in safety-critical, high-integrity communication, only layers one, two, and seven of Fig. 2.1 are present. Some of the lower layers functions (1–6) can be handled at the application layer (7) using application-specific methods. Systems conforming to an established protocol (like PROFIBUS) are more likely to have application independent layers of software (communication stacks) and hardware (ASICs).

The reduced layer model is shown applied to a safety system in Fig. 2.3.

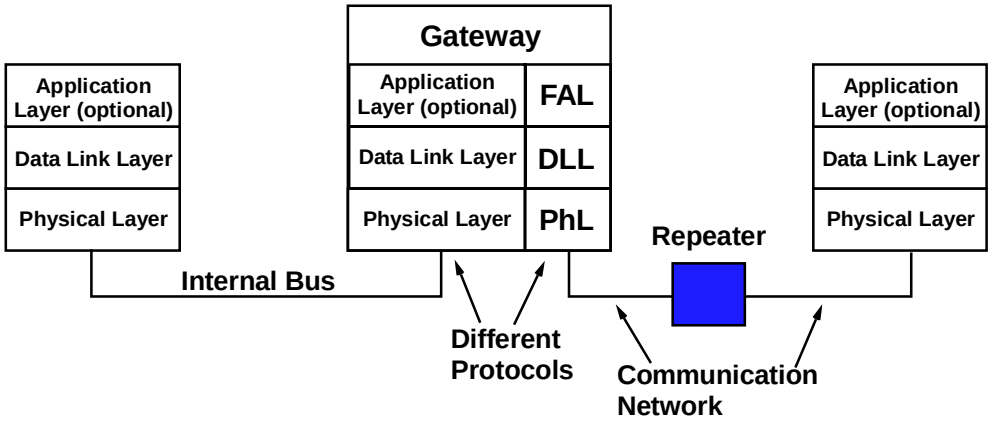

Fig. 2.3. Three-layer model applied to a safety system network. Note that the gateway and repeater are present as examples.

A network's topology is determined on the basis not only of the communications paths needed for the application, but also by its reliability, safety, and availability needs. A safety system's network topology can have aspects included specifically to increase the reliability of the network. A topology can include redundant, even diverse, links to provide

1. fault tolerance by providing a functioning link,
2. fault detection through the comparison of transmissions received through multiple links, and
3. fault removal by automatically reconfiguring transmission paths around failed links.

Other examples are topologies that provide

1. fault tolerance through the use of isolation equipment or protocols that limit the extent and propagation of a fault, and
2. fault removal through fast recovery after a fault.

Example redundant topologies are shown in Fig. 2.4. Further information on network redundancy is available in Refs. 1 and 2.

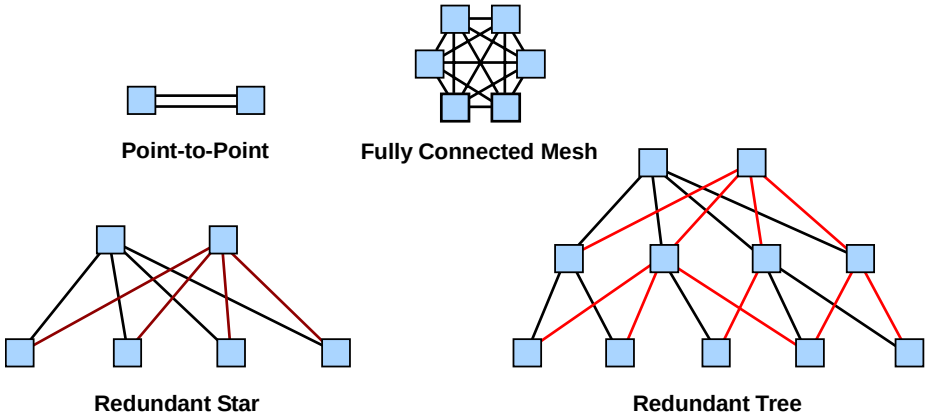

Fig. 2.4. Communication networks with redundant topological features applicable to safety.

Network topology can change with system operating modes. For example, while in maintenance mode, new links as well as new nodes may be added that fundamentally alter the characteristics of the network's operation. Network security and reliability relies in part on control over the network's topology. If the topology can be altered, then security and especially reliability might be compromised. Nonconstant topologies make comprehensive testing very difficult.

The National Research Council[3] suggests that point-to-point data links in the plant's protection system will provide more deterministic and predictable data communications. Fewer data points are normally needed by safety systems (as compared with plant control systems). Improved reliability comes about because of simple node structure and little data collision potential. Whatever topologies become implemented, whether bus or point-to-point, need to be designed to ensure performance, reliability, and failure states within the design basis requirements of the protective system. This is true.

Messages are sent between nodes using methods to ensure correct routing, scheduling, authenticity, and data integrity. The message source can add to the primary data information that indicates a unique serial number, a recipient identifier, the time of origination, the sender identifier, and a corruption detection key. Other information may also be added by routers and the action of communication layers. Several of the standards discussed in Sect. 4 go into detail as to preferred protocols for message construction.

2.2 GENERAL NATURE OF DIGITAL COMMUNICATION ERRORS

Communication is about the delivery of information from a source to one or more receivers and the delivery of a response from the receiver(s) to the source, showing how the information was received and used. In a world without bandwidth limits, noise, transients, and errors, information would be correctly assembled and coded at the source and transmitted to the receiver; at the receiver that information would be decoded and used properly. Unfortunately, failures and errors can appear in various places along the path from source to receiver. Possible error sources include the following:

1. source-generated errors,
2. errors generated in the communication/transmission channel,
3. receiver-generated errors, and
4. system-wide, component interaction generated errors.

In general, two broad classes of communication failure apply to safety systems: (1) information failure and (2) transmission failure. Information failure refers to errors that end up affecting the message or errors that delay the message so that it is no longer useful. Transmission failure refers to the complete loss of information. No condition or event related to external communications should alter execution of the safety function. This refers to communication network events such as loss of data or abnormal plant events.

2.2.1 Error Types

A nonexhaustive list of communication error types has been compiled from several sources.[4,5] The errors are divided into two categories according to whether the error is predominantly communication channel related or is associated more with message sender or receiver. These error types also correspond to the failure modes that the National Research Council[3] considered associated with digital communication systems.[*] The National Research Council report also suggested considering failure modes associated with shared resources such as multiplexers.

The first category of error type is predominantly communications related as shown in Table 2.1. These errors are described in the paragraphs that follow.

Table 2.1. Communications-related errors

Corruption
Unintended Repetition
Incorrect Sequence
Loss
Unacceptable Delay
Insertion
Masquerade
Addressing
Broadcast Storm

Corruption—Messages may be corrupted because of errors in communications processors, errors introduced in buffer interfaces, errors introduced in the transmission media, or from interference. The occurrence of message errors during transmission is a common event for standard communication systems. Cyclic redundancy checks (CRCs)[†] offer a high probability of error detection in receivers. Typically, communication systems include protocols for message error recovery; not all corrupted messages end in data loss unless recovery or repeat transmission procedures either fail or are not employed. The latter would be the case for unidirectional transmissions from a safety system.

[*]From the National Research Council report: "Failure modes associated with communication systems include (a) lost and late messages; (b) misdirected messages; (c) messages that lose meaning after being sent because the sending processor rolls back to a previously saved check-point owing to an error (commonly known as orphan messages); and (d) inconsistent messages to other processes, which can cause the receivers to act inconsistently (commonly known as Byzantine messages)."

[†]A CRC takes a data stream as input and produces a fixed-length output value. A CRC can be used in the same way as a checksum to detect data alteration. CRCs, which are simple to implement, are especially effective at detecting common errors caused by transmission channel noise. However, a checksum does not provide the same protection for detection of bit errors.

Unintended Repetition—Messages (old) may be repeated at an incorrect time due to an error, fault, or interference. Sender retransmission is a typical procedure when an expected acknowledgment is not received from a target receiver. The receiver, also, can request a retransmission when a missing message is detected. Some protocols use multiple transmission of the same message to increase the probability of uncorrupted reception.

Incorrect Sequence—Predefined message sequences (such as process variables and time references) associated with a series of messages from a particular source may be incorrect because of an error, fault, or interference.

Loss—Messages may be lost because of an error, fault, or interference. The loss includes both failures to receive and acknowledgment of received message.

Unacceptable Delay—Messages may be delayed beyond their permitted arrival time window. Conditions leading to delays include errors in the transmission medium, congested transmission medium, interference, and delay in sending buffered messages.

Insertion—Messages may be inserted into the communication medium from unexpected or unknown sources. These messages are in addition to the expected message stream. They cannot be classified as Correct, Unintended Repetition, or Incorrect Sequence because the sources are not expected.

Masquerade—Invalid messages may masquerade as valid ones from an expected source. Communication systems used for safety-related applications may employ further checks to detect Masquerade, such as authorized source identities and pass-phrases or cryptography. This error type applies to any extra-division communication across a multinode architecture (e.g., operator's station to multiple divisions).

Addressing—A safety-relevant message, due to a fault or interference, may be sent to the wrong safety-relevant destination. The receiver could treat the message as a valid communication.

Broadcast Storm—A condition in which a message that has been broadcast across a network results in even more responses, and each response results in still more responses in an increasing progression. Responses from receivers may be nearly instantaneous or delayed. The storm may be not deliberate or malicious in intent. A severe broadcast storm can block all other network traffic, resulting in an unresponsive network. Storms can occur if network equipment is faulty or configured incorrectly, for example, if the Spanning Tree Protocol[*] (or its equivalent) is not implemented correctly or if poorly designed programs that generate broadcast or multicast traffic are used. Broadcast storms can usually be prevented by carefully configuring a network to block illegal broadcast messages or by removing unused functionality. An example of a broadcast storm and its consequences is given in NRC Information Notice 2007-15.[6]

The second category of error type is more closely associated with source and receiver function as shown in Table 2.2. Descriptions of the errors are provided in the following paragraphs.

Table 2.2. Sender- or receiver-related errors

Buffer Overflow
Data Out of Range
Incorrect Ordering

Buffer Overflow—Messages may be longer than the receiving buffer, which results in buffer overflow and memory corruption. Such an overflow could occur at any data layer.

[*]The Spanning Tree Protocol (STP) is defined in the IEEE Standard 802.1D. As the name implies, it creates an interconnected tree graph within a mesh network of connected layer-2 bridges (e.g., Ethernet switches), and disables the links which are not part of that tree, leaving a single active path between any two network nodes.

Data Out of Expected Range—Messages may contain data that are outside the expected range for the given data type. Examples are incorrect times and process variables.

Incorrect Ordering—Messages may appear valid, but data may be placed in incorrect locations within the message. Some communication system structures may assemble a complete message sequence by concatenating elements stored in disparate memory locations. The final sequence may be incorrect because of a deviation in the assembly order or incorrect data in the associated memory locations. A twist on the Incorrect Ordering error type is inadvertent mixing of engineering units because of an error resulting from extracting data from an incorrect memory location. In this case, the messages may appear valid, but data are in unexpected units [such as International System of Units (SI) vs U.S. customary units]. This example was taken from the September 1999 NASA Mars Climate Orbiter crash that resulted from a failure to convert English units into metric units in a segment of the orbiter's navigation-related software.

Besides the error categories described above, two additional error categories may apply to networks that contain bridges or routers:

- very long delays in bridges and routers, and
- very long times to initiate communications.

Bridges may store safety-related messages for a period before transmission to the next network. This design issue must be evaluated if bridges and routers are used between nonsafety and safety systems.

A comparison of error types with the three primary communication layers (see Fig. 2.3) is shown in Table 2.3. The analysis shown is not complete but illustrative of the relationship between error categories and the domains of the communication layers. An evaluation of a digital safety design should include a determination as to whether these errors can detrimentally influence the functioning of a safety system.

Table 2.3. Comparison of communication error types with the three primary abstraction layers

Communication layer[a]	Error category							
	Corruption	**Unintended repetition**	**Incorrect sequence**	**Loss**	**Unacceptable delay**	**Insertion**	**Masquerade**	**Addressing**
Application *Layer 7*	Message handling flaw can result in corruption	Applications might send message > 1 time due to flaw	Applications might have responsibility for sending some types of messages first	Flaw could cause loss	Flaw could cause delay			Applications can be responsible for node names that are ultimately translated into network addresses
Data link *Layer 2*	Handles or introduces corruption	Handles or introduces unintended repetition	Handles or introduces incorrect sequences	Flaw could cause loss	Flaw could cause delay	Flaw could cause insertion	Flaw could cause masquerade	Sends the message on the wrong communication port[b]
Physical interface *Layer 1*	Corruption within the physical media			Loss within the physical media	Flaw could cause delay	Flaw could cause insertion	Flaw could cause masquerade	Connected to the incorrect destination[c]

[a] See Fig. 2.1

[b] Error could occur if the application making the port decision is flawed and the computer has multiple ports. Under rare circumstances, error could occur and, therefore, might not be discovered by testing.

[c] This is not the type of error that should happen after a reasonable test of the system because all messages would be affected.

2.2.2 Message Types Relevant to Safety Applications

Message data sent or received by a safety system across a network connection can be classified according to its use. The six categories of message types are shown in Table 2.4. These data types are described in the subsequent paragraphs.

Table 2.4. Message data types by purpose

Software Coding (Programming Updates)
Set Points and Parameters
Command Functions
Go/No-Go (Interlocks)
Data Transfer
System Status

Software Coding (Programming)—The digital processors in safety and communications systems utilize microprocessors to carry out the instruction sets stored in memory. Periodically, updates in the software coding are necessary to fix bugs, vulnerabilities, and implement improvements. For nonsafety systems, the transfer of executable software coding modifications, updates, and sometimes all new programming to the system, may be accomplished over communication networks. Obvious error entry points are incorrect binary values in the data stream and misdirected modifications. For safety-critical applications, it is more appropriate to supply a dedicated means of modifying executable code such as full manual replacement (on the circuit board) of nonvolatile memory that holds the coding. Although dedicated bus or network may have economic benefits for programming changes, for safety-related systems, such reprogramming should be permitted only on dedicated communications pathways not associated with common (safety) data transfer. (The TELEPERM™ system uses Ethernet for maintenance functions and PROFIBUS for safety functions.)

Set Points and Parameters—Although the transfer of new operating set-points or safety-system operating parameters to a system may be necessary during the course of normal plant operation, such network communications should be kept to a minimum. This type of communication may contain digital representations of analog gain values or filter settings. An example is sending gain adjustments from the nonsafety core monitoring computer to the safety-related power range neutron monitoring system in a boiling-water reactor. These parameters could be directed to an incorrect digital subsystem or received as an instruction by an incorrect digital subsystem. In addition, parameter values can be corrupted and misinterpreted. After data are loaded, a confirmation process with corroboration and identity proof of decision-maker is often used to reduce errors in transmission.

Command Functions—A command instruction contains more data than the Go/No-Go instruction and is more extensive. A sequence of events may be described in the command. A complete command sequence may comprise several message sets. A command directive to execute or stop executing function(s) may contain multiple parameters. An example is to instruct a major system to enter a different operating mode. Similar to the Go/No-Go instruction, a source of error for the command instruction is the misdirection to an incorrect digital subsystem or reception as an instruction by an incorrect digital subsystem. The communications channel may be compromised.

Go/No-Go (Interlocks)—Simple command-like instructions to enable or disable a software or hardware function are needed for operations such as interlocks. A Go/No-Go instruction is by nature discrete binary—has two ultimate states. The communication message instructs the system to one of the states such as permitting another station to talk. The Go/No-Go instruction should never toggle between states because the latter state becomes dependent on the previous state and therefore may be uncertain. The Go/No-Go instruction is absolute. An obvious error can occur should the command be

directed to an incorrect digital subsystem or received as an instruction by the incorrect digital subsystem.

Data Transfer—The timely flow of data between safety systems, or between safety and nonsafety systems, is needed communicate measured nuclear and process values, trip calculation results (which are associated with trip variable—binary in nature), and operability status for other safety divisions. The timing requirements must be met under all plant conditions (e.g., a plant event that generates many alarms), and for all permissible states of the network (e.g., one node is in maintenance mode). Safety and nonsafety displays and other nonsafety data consumers can be designed for a periodic, controlled data flow, which sets the total throughput requirements. In a completely deterministic safety-system network, data are acquired by a periodically dispatched task and thus should be sent only when the periodically dispatched task completes and provides a new data set. However,a network's design might be deterministic in normal operation but also use some nondeterministic behaviors such as retransmission for error recovery or system maintenance mode. In all cases, the network must provide timely access to sufficient bandwidth to meet the needs of all of the systems on the network. Data transfer for a safety-critical digital system (input or output) should never exceed bandwidth capacity of the operation. In nondeterministic networks, live or real-time streaming of multiple system values (e.g., data for operator displays) may require extensive transmission of system variables, parameters, set points, and status conditions; all of which can consume network bandwidth

System Status—The current state of a system or component may be communicated as a periodic, controlled data flow, in a deterministic network or as a short burst of data in a nondeterministic one. Status information is limited to a small set of indicators that can be requested or transmitted periodically without request. An example might be a periodic communication to a visual display unit, indicating safety system status. Multiple requests to supply status information might flood the network and slow down communication system response. Design configuration should preclude the physical possibility of communications systems being overwhelmed to the point of denial-of-service. For example, establish a limitation on the number and types of requests that can be issued during specific periods. Repeated requests for the same data over a certain reasonable period should be prohibited. An undetermined minimum and maximum periodicity for reporting is a distinct liability.

Errors and mitigation methods related to the message types described above are listed in Table 2.5. These methods are illustrative only because there are many ways a designer can develop a system.

Table 2.5. Message types and error effects

Message type	Description	Communication example	Potential detrimental effect of error	Possible methods to mitigate effect[a]
Software Coding (Programming)	Transfer of executable software coding modifications, updates, or all new programming to the system. (Note that the prevalent method of changing software coding in safety systems is manually to replace nonvolatile memory on the circuit board.)	Software or firmware upgrade to correct a bug or vulnerability	Software could be directed to an incorrect digital subsystem or be incorporated in the incorrect subsystem	Programming changes permitted only on isolated communications pathways or buses not associated with other common data transfer. This transfer should be on a separate network from the deterministic data paths used for safety- and nonsafety-related data transfers. Administrative protection is required. Transfers should only occur while the system is not credited with performing its safety function

Table 2.6. (continued)

Message type	Description	Communication example	Potential detrimental effect of error	Possible methods to mitigate effect[a]
Set Points and Parameters	Transfer of new set points or operating parameters to a system. Communication contains analog values such as temperatures, pressures, filter settings, etc.	Change of safety system trip-threshold value. Plant example: gain adjustments from the nonsafety core monitoring computer to the safety-related power range neutron monitoring system in a boiling-water reactor	Set point values could be directed to incorrect digital subsystem or received as an instruction by the incorrect digital subsystem. Partial information may be incorporated and action taken	Execute edit/confirmation process after data are loaded, that is, separate, deliberate process with corroboration and identity authenticity of sending system. Permit set point changes over controlled and limited node network
Command Functions	Directive to execute or stop executing function(s) potentially with multiple parameters contained in the communication. More extensive than the simpler go/no-go command	Enter a different plant operating mode	Command could be directed to incorrect digital subsystem or received as an instruction by the incorrect digital subsystem. Communications channel may be compromised	Execute edit/confirmation process after commands are loaded and identity authenticity of sending system. Limit crucial commands to point-to-point network, which includes some ring type networks. Lockouts may prohibit more than one safety node at a time from using the bus
Go/No-Go (Interlocks)	Simple discrete command to enable or disable a software or hardware function	Set a digital system in bypass	Command could be directed to incorrect digital subsystem or received as an instruction by the incorrect digital subsystem	Execute edit/confirmation process for message and identity authenticity of sender. Limit crucial interlocks to point-to-point network
Data Transfer	Transmission of extensive system variables, parameters, set points, and status conditions. Could contain historical, current, and predicted data. In a nondeterministic network, the stream may be requested or sent periodically. In a deterministic safety-system network, data are transferred periodically when the periodically dispatched task completes and provides a new data set	Response to a command for detailed operating set points and plant variables. Plant example: measured nuclear and process values and trip calculation results	Consumes network bandwidth—bandwidth usage is variable on a nondeterministic network and can lead to network choking. Reporting by exception rather than a fixed report of all values without exception can lead to network overload and loss of data.[b,7] (Note that display of an extensive list of reactor system data-elements represents an inherent risk for operator overload.)	Buffering between safety processor system and communication system necessary to prevent challenging of the safety processor. Data transfer for a safety-critical digital system (input or output) should never exceed bandwidth capacity of the network. Control of bandwidth can be enforced by deterministic methods such as periodic reporting of all values. Such communication networks should be analyzed for periodic, controlled data flow, which sets the total throughput requirements

Table 2.6. (continued)

Message type	Description	Communication example	Potential detrimental effect of error	Possible methods to mitigate effect[a]
System Status	Short burst of data indicating current state of reactor or digital system. Status is limited to small set of indicators or block of indicators. Status may be requested or transmitted periodically without request	Periodic scheduled communication indicating safety system status	Request if not scheduled on the same periodic basis as data sampling and logic solution could consume bandwidth. If the status data are scheduled, there is no need for a request. Multiple requests on a nondeterministic network might flood the network and slow down system response	Buffering between safety processor system and communication system necessary to prevent challenging of the safety processor. Design configuration should preclude the physical possibility of communications systems being overwhelmed to the point of denial-of-service. This is accomplished by using a deterministic network. Otherwise, establish a limitation on the number and types of requests that can be issued during specific periods. An undetermined minimum and maximum periodicity for reporting is a distinct liability. Repeated requests for the same data over a certain reasonable period should be prohibited

[a]The methods of mitigation suggested in this column serve as examples not absolute requirements.

[b]With its complex, fully redundant communication links and shared communication links between safety and nonsafety functions, the P20 architectural design was extremely ambitious in light of the available technology. It was found that a communications-by-exception approach employed for some parameters created the potential for communication saturation of cluster interfaces (i.e., "choke" points) during off-normal events. While this response characteristic might have been addressed through design modification, the regulatory authority was concerned that the Class 1E functions could not be qualified without major design changes.

REFERENCES

1. K. Burak, "Ethernet Redundancy," presented at ANS 5th International Topical Meeting on Nuclear Plant Instrumentation, Controls, and Human Machine Interface, Albuquerque, New Mexico, November 12–16, 2006.
2. L. Meter, "Invensys Solution for a Complete Digital I&C System Upgrade for a Nuclear Power Plant," presented at ANS 5th International Topical Meeting on Nuclear Plant Instrumentation, Controls, and Human Machine Interface, Albuquerque, New Mexico, November 12–16, 2006.
3. "Digital Instrumentation and Control Systems in Nuclear Power Plants: Safety and Reliability Issues (1997)," D. M. Chapin (Chair), http:llwww.nap.edulopenbookl03090573291htmllR2.html, Final Report 1997, The National Academy of Sciences, National Academy Press, Washington, D.C.
4. J. A. Lenner, "The Development of Safety Networks in a 61508 Environment," presented at ISA Expo 2003, www.isa.org.
5. IEC 61784-3/CDV, "Digital Data Communications for Measurement and Control," International Electrotechnical Commission, draft version 4.0.
6. NRC Information Notice 2007-15, "Effects of Ethernet-Based, Nonsafety Related Controls on the Safe and Continued Operation of Nuclear Power Stations," April 17, 2007, NRC Technical Contact Royce Beacom, rdb1@nrc.gov.

7. R. T Wood et al., *Advanced Reactor Licensing: Experience with Digital I&C Technology in Evolutionary Plants*, NUREG/CR-6842, April 2004.

3. INTERNATIONAL NUCLEAR STATION REVIEW

3.1 INTERNATIONAL SAFETY CLASSIFICATION SUMMARY

Different nuclear power regulatory bodies employ different safety-system classification schemes. The United States employs a two-level classification scheme (safety and nonsafety) or more precisely, Class 1E and non-Class 1E. Class 1E is defined by function in IEEE-603[1] as

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

All other nuclear safety bodies employ a more finely graduated safety classification system. The International Atomic Energy Agency (IAEA) has basic safety requirements for design (IAEA NS-R-1)[2] that creates a two-subclass safety class. IAEA Safety Guide 50-C-D[3] provides the IAEA safety grading scheme, including providing examples of classification of major NPP systems and components. IAEA Safety Guide NS-G-1.3[4] applies this classification scheme to NPP I&C systems. The IAEA subdivides its safety class into safety systems and safety-related systems. Safety systems are limited to those components that ensure reactor shutdown and residual heat removal from the core as well as those systems that limit the consequences of anticipated operational occurrences and accident conditions. Safety-related I&C systems perform all other safety functions than those called out in the safety requirements for design.

IEC 1226[5] presents a similar safety classification system. The standard identifies three I&C categories for systems that are important to safety. Category A refers to functions, systems, and equipment that have a primary role in the achievement or maintenance of NPP safe conditions. Category B refers to functions, systems, and equipment that support Category A systems. Category C is assigned to functions, systems, and equipment that have an auxiliary or indirect role in the achievement or maintenance of NPP safe conditions.

IAEA-TECDOC-1066[6] provides a safety classification table (modified with additions as Table 3.1) that illustrates the comparative safety classification and categories employed in different NPP I&C systems. Table 3.1 is intended to illustrate the general international safety categories and does not represent precise relationships among the various categories in the standards. Note that non-Class 1E safety classes are not unregulated and indeed require high levels of quality. Non-U.S.

Table 3.1. Comparative NPP I&C safety classifications

National or international standard	Safety classification grade				
IAEA	Systems important to safety				Systems not important to safety
	Safety system		Safety-related system		
IEC 1226	Category A		Category B	Category C	Unclassified
France N4	1E		2E	Important for safety/nonclassified	
European utility requirements (EUR) (time dependent)	F1A (automatic)	F1B (automatic and manual)	F2		Not classified
UK	Category 1		Category 2		Not classified
USA (IEEE)	1E		Non-nuclear safety		
Finland	SC1	SC2	SC3	SC4	EYT
Hungary	ABOS 2	ABOS 3	Unclassified		

nuclear regulatory authorities have allowed communication and commands to pass between different levels of safety systems. However, no nuclear power regulatory authority has permitted two-way communication or command of the highest class of safety systems from nonsafety classified systems.

3.2 INTERNATIONAL NUCLEAR PLANT EXPERIENCE

This section addresses the safety and reliability issues of communications within digital protection systems of international reactors. Any protection system, digital or analog, is composed of many individual components that communicate with each other to measure the status of the plant, execute the logic of the protection system, and take appropriate action. In traditional analog systems, the communication is simply point-to-point wiring that carries a voltage or current between components. Point-to-point wiring of analog signals still comprises a significant fraction of the communications within a digital protection system because many of the sensors are analog transducers. The licensing concern for analog wiring in the digital protection system is no different from that for an analog system. However, with the introduction of digital systems, time multiplexing of binary values has been introduced that can convey a great deal more information over a single wire than an analog system.

To illustrate the types of communication in a microprocessor-based system, consider the generic rack of components illustrated in Fig. 3.1.

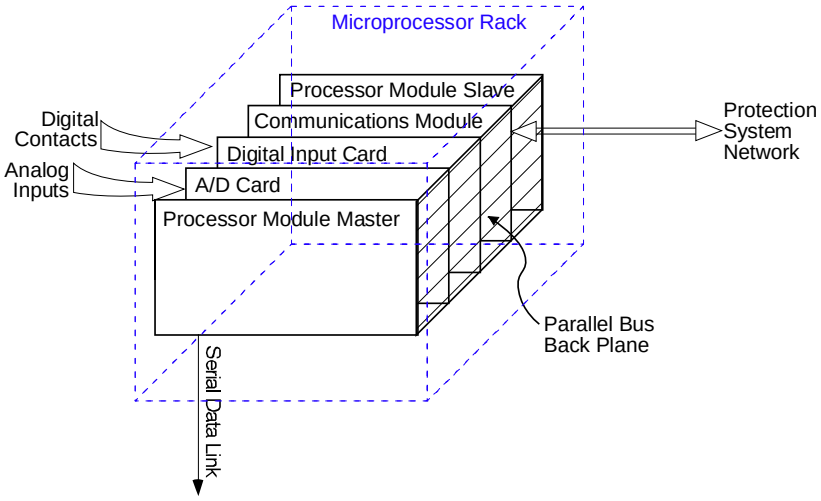

Fig. 3.1. Generic microprocessor-based rack.

Three digital forms of communication can be identified within a typical digital protection system:

Bus Communication: This connection is commonly used with multicard computer systems and consists of an array of parallel conductors forming a signal bus. Usually, one module, the master processor, is the bus master and controls which module can put information on the bus. A motherboard may have several buses. A number of standards exist such as IEEE 796 or VMEbus or other commercial bus architectures to define the bus and interactions of components. This type of communication typically exists only within a single division of a safety system. The main advantage is high-speed data transfer.

Serial Communication: This type of communication is commonly used to connect individual digital devices together and may be conducted through a point-to-point wire or optical fiber. Information is encoded as a string of binary pulses that follow a standard scheme such as Manchester or nonreturn to zero encoding. For automation and control, most communications between the

computing level of the system and the sensing and actuation level take place as a serial communication. The information on a serial bus tends to be very specific to the device and fixed in format. Error checking is applied to validate the message. Because a single connection can contain multiple signals, the design of the system must ensure that a serial link is not a point of single failure for a particular safety function. Serial data links may communicate between devices within one division of a safety system or between two divisions or between safety systems and nonsafety systems. The requirement for communications that cross division boundaries is that the channel is electrically isolated and can continue to execute its safety function(s) despite a failure of the communications link or the system sending the message. Although standard serial communications protocols provide for bidirectional transfer, bidirectional transfer clearly poses a vulnerability in protection systems. Most existing systems use two one-way serial connections to implement bidirectional information flow when needed.

Network Communication: The network communication is serial in nature but allows messages to be addressed to many receivers. Protection systems have drawn on commercial standards such as token ring networks and Ethernet. In some instances, the safety system communication is connected to a nonsafety-grade network through safety to nonsafety isolators. In other instances, the network is a safety-grade system. Some of the general purpose features commercial network protocols have to be altered or removed to reach the high level of security and testability required for safety system applications. A general purpose network is not a deterministic message system and provides for random generation of messages. This leads to a potential for uncertain timing between sending and receiving as well as the loss of a message. For token-passing networks as an example, the network is under control of the last token holder. Safety-grade networks use commercial hardware but modify the network software to ensure that the communications are deterministic and timing is fixed.

The network communications are used in safety systems to communicate large blocks of data for applications such as operator consoles, data historians, and postaccident monitors that require bringing many inputs together in a single device.

Fig. 3.2 shows a typical arrangement of digital components for a channel protection system. The main protection functions are signal input, comparison (and potentially other computations), voting, and connection to the actuated devices. These four functions are shown implemented in three modules. The modules communicate via a parallel bus in the backplane. The banks of these modules communicate by a serial connection that emulates a backplane. A failure of the communications at any interface within the sequence of modules forming the primary functions results in a failure of the channel. Channel failure is addressed by the redundancy of the channels and the voting scheme. Because the connections between modules and racks are point-to-point and carry specific data, the analysis of failures of these communications is much like conventional wiring. Multiple values are concentrated on the single connection, but the situation is not inherently different from multiple conductors in a single cabinet of a safety channel division. Tests to determine functionality are built into the communication (like checksum and watchdog timing).

Additional functions of the safety system such as communication to the plant control system and to nonsafety display systems, signal validation, or test and maintenance are handled by separate modules that utilize network communications. Network communications are shown as a broader line connecting to the sides of the racks. The architecture is designed to handle a failure of the network so that the main protection function continues whether the network or any component on it fails.

This report is mainly concerned with communications that involve cross division boundaries or that connect between a safety and nonsafety system. Communications within a single division do not introduce pathways for propagation of failures among divisions. A communication failure within a channel resembles the single random failure modes of a conventional system and is addressed by the single failure criterion. A greater concern is a connection that may affect the independence of channels and divisions. Some general categories of communications links follow.

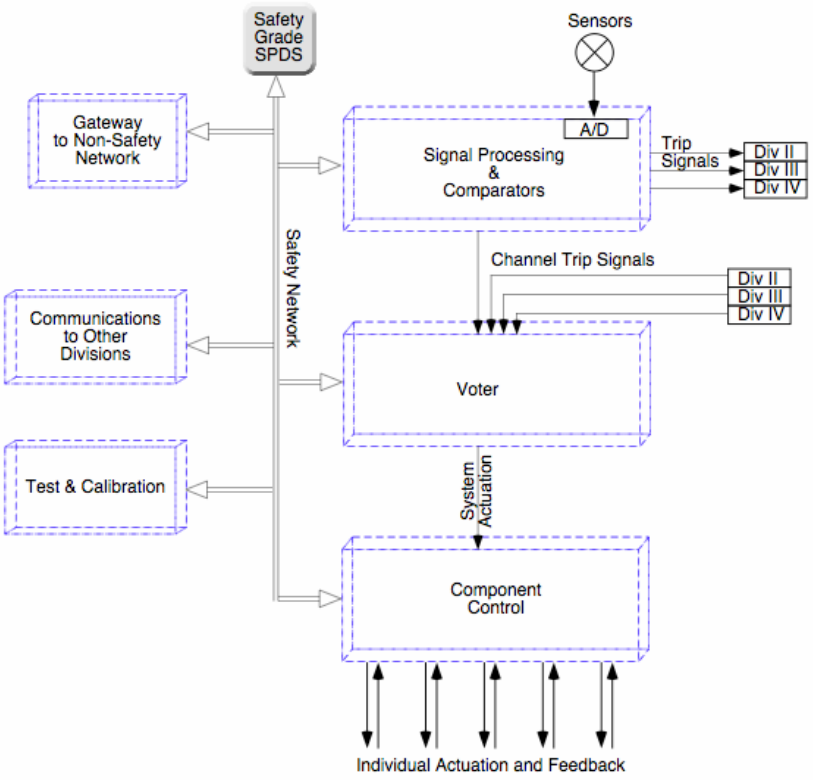

Fig. 3.2. A representative arrangement of modules in a digital protection system.

Division to Division: New interdivision communication has been introduced in some digital system communications for purposes other than voting. Voting requires communication of the division's trip status to a voter device and is equivalent to analog systems in this regard. Redundancy built into digital systems' voting schemes is similar to analog voting of previous generations and has the same degree of protection from single failures. The logic for most systems is two-out-of-four. In digital systems additional communications have been added to enable enhanced functionality, such as signal validation and automatic calibration features that may require additional interdivision communication of sensor and/or bypass information. The impact of these latter types of communication on division independence must be carefully considered.

Safety to Nonsafety: These communications typically include transmission of signals by the safety system. Examples include measured sensor values, internal status, and trip status outputs from the safety system for display or control. Typically, data handling systems such as the postaccident monitoring system, safety parameter display system, plant computer, or operator console that display and store data from the protection system are not safety grade. The plant control system may use either sensor data or an output from the safety system. The concern of safety to nonsafety communications is isolation to protect the propagation of a fault from a nonsafety system to a safety system.

Nonsafety to Safety: Typically, no communications of this type are allowed in the international reactors studied. This review looked for any exceptions or unusual instances that could fall into this category. The only instances include second-tier safety features in a foreign licensing hierarchy that would be considered nonsafety under U.S. nuclear code or manual controls for dual-use components such as pumps in the Engineered Safeguards System that are used both for safety injection and for chemical and volume control. Typically, for dual-use components, a component interface device

receives safety, nonsafety (control), and manual inputs and prioritizes the signals. The device is located immediately upstream of the final actuation hardware.

3.3 DESCRIPTIONS OF DIGITAL COMMUNICATIONS ARCHITECTURES IN INTERNATIONAL REACTORS

Individual implementations of digital protection systems differ in details and specific features from the hypothetical example given in Sect. 1. The following discussion gives a number of specific examples of digital protection systems in international reactors. The goal is to identify (a) the locations of communication links, (b) the technology involved, (c) any segregation strategy for functional diversity in which certain portions of the protection are not permitted, (d) any communication link to preclude communication-based failure, and (e) to discuss any hardware or software features of the communications links that are designed to limit the type or severity of failures. The main concern is a common cause failure mechanism involving the communication. The information that can be found is used to identify the types of communication used between the main components at different levels, the physical media such as copper or fiber optic cable, the communication protocol, and any special design features that enhance reliability or eliminate a potential common cause failure. When communications between the divisions of the safety system and between the safety system and the nonsafety systems are permitted, the report describes methods to ensure electrical, communicational, and functional isolation of the systems. The review addresses the strategies of different vendors to ensure overall reliability of the communications system so that failures rates of individual links are very low and to ensure that there is no common cause failure in the communications systems that compromise the function of the safety system.

3.4 CHOOZ B (FRANCE)

The first generation of digital protection systems in French pressurized-water reactors (PWRs) (known as SPIN P4[*]) was installed on all 1300-MW(e) nuclear power plants. Paluel 1, the first of the P4 type, was connected to the grid at the end of 1984. The operating experience gained from these digital protection systems was used in the design of an upgraded version of protection system equipment (SPIN N4) installed on the N4 plants [1500-MW(e) units (Chooz B 1 and 2 and Civaux 1 and 2]. Digital protection system technology has undergone further improvement in the development of SPINLINE 3. The basic evolution in the architecture may be summarized as follows:

Year ~ 1980s: 1300-MW(e) Plants (e.g., Paluel 1-4): Used SPIN P4 protection system technology; 8-bit microprocessors (Motorola 6800); point-to-point links between subsystems; assembly language programming; RAM memories supporting time-dependent variables; PROM memories containing non-modifiable data; REPROMS containing programs and modifiable data; fiber used for data transmission, when electrical isolation is necessary.

Year ~ 1990s: 1400 to 1500-MW(e) plants (e.g., Chooz B 1, 2; Civaux 1, 2): SPIN N4 protection system technology; 16-bit microprocessors (Motorola 68000); C language for programming; use of computer-aided software engineering (CASE) tools; use of system networks.

Year ~ 1997: 900 MW(e): SPINLINE 3 protection system technology; 32-bit microprocessors (Motorola 68040); C language programming; use of CASE tools; use of system networks.

Year ~ 2007 to present: TELEPERM XS protection system technology; use of 32-bit processors; C language programming; use of CASE tools; use of system networks.

[*] SPIN is a French acronym for digital integrated protection system and reflects an integrated reactor protection and engineered safety features system.

The following are the safety classes used in the N4 I&C architecture (Fig. 3.3) as well as their descriptions:

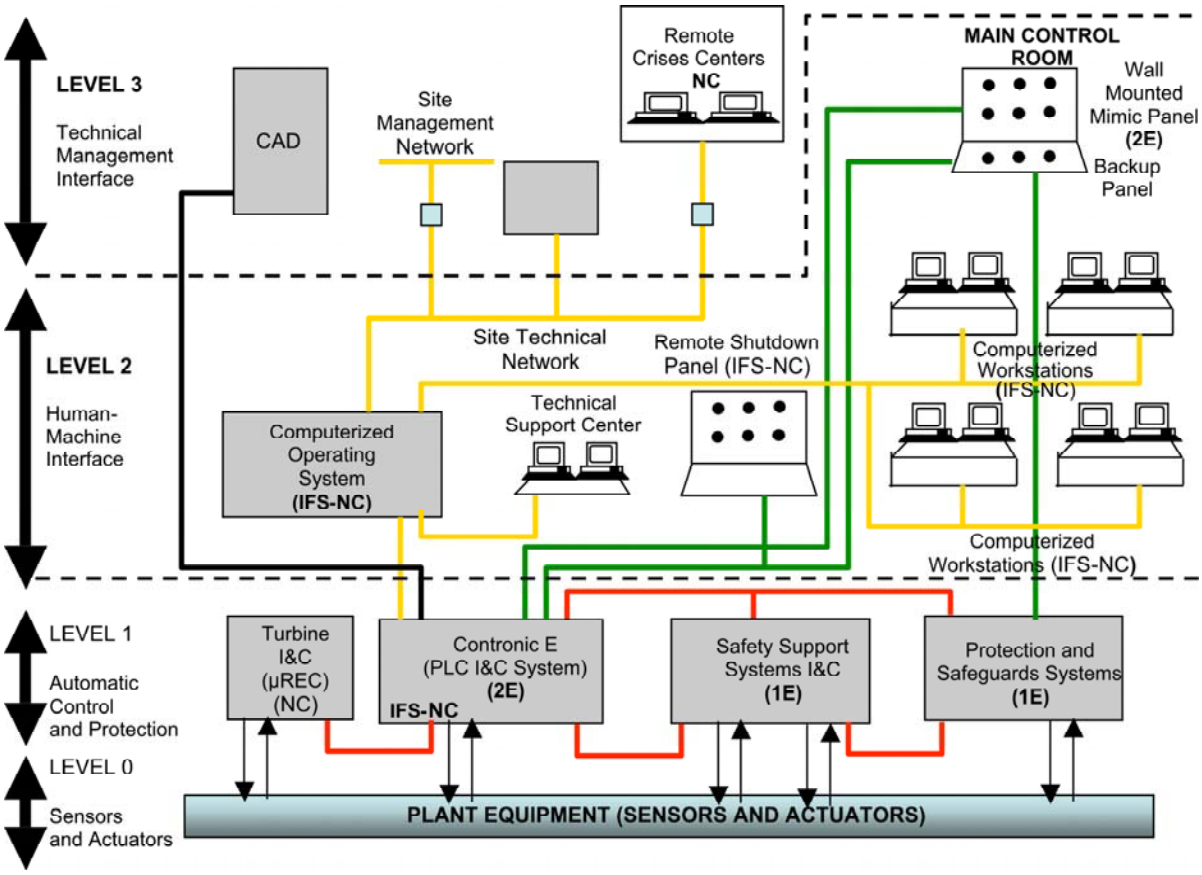

Fig. 3.3. I&C architecture of Chooz B (N4) Plant.

Class 1E (Safety System): Functions involved in the short-term phase following an accident or to return the unit to a safe and stable state, such as reactor trip (e.g., SPIN N4 protection system). This is the highest safety class. Equipment designated as Class 1E must meet requirements related to redundancy (single-failure criterion), redundancy in power supply, physical and electrical separation, equipment qualification (environmental and seismic), periodic testing, RCC-E rules on design and construction, and other French quality regulations. In addition, if software is involved, it must meet the requirements of IEC 60880 and other software qualification criteria.

Class 2E (Safety-Related System): Functions involved in the medium and long-term phases following an accident. Includes manual actions performed by the operator in order to remain in the safe state or to return to the fall back state. An example is the manually operated shutdown system. Equipment designated as Class 2E must meet requirements related to redundancy (depending on the particular application), alternative power supplies, equipment qualification (environmental and seismic), periodic testing, RCC-E rules on design and construction, and other French quality regulations.

IFS-NC (Important for Safety—Nonclassified): Other safety functions that are not directly involved in the safety demonstration and are useful but not indispensable or the failure of which must be examined from the safety aspect. Examples are the operator workstations.

NC (Nonclassified): Other functions that are not in any of the categories above.

SPIN contains internal network interconnections using a dedicated Ethernet-based protocol. Only point-to-point communication links exist from non-Class 1E systems/components to Class 1E systems/components. Communications that go from less classified systems to 1E systems are 4-to-20-mA current loops or discrete inputs (most of these links communicate discrete states representing on/off status of a piece of equipment). The maintenance terminal uses a serial link. The maintenance terminal is only connected when in use for maintenance operations.

In N4, nearly all 1E functions are completely automatic. The few manual operations are hardwired in the PIPO, which is 1E, classified: no soft control is provided (hardwired manual is provided). The design is a result of the definition of the 1E class, which is defined as the set of mitigating functions necessary within the first 30 min after an initiating event. During this time, the operators do not need to actuate anything (with very few exceptions) to ensure the safety of the plant. This interval is provided so that operators may gather information to understand the situation and define their strategy.

The N4 control room has three operator interface stations:

- The main control panel (the KIC[*]) is classified IFS-NC. It can actuate NC, IFS-NC equipment, and 2E equipment through the SCAT[†] (which is 2E classified). The KIC cannot actuate 1E equipment.
- The Auxiliary Panel is classified 2E. It can actuate NC equipment, but not 1E equipment.
- The PIPO is classified 1E. It can actuate 1E equipment.

The communication paths from the control room down to actuators for nonsafety automatic or manual control inputs to the nonsafety actuators travel from Level 2 in the plant computer through the network to the level 1 local controller. Those signals that actuate dual-use, safety and nonsafety components pass down to the priority module on the actuator electrical cell. The priority module consists of relay-based logic to arbitrate safety and nonsafety inputs to the actuated device. Diverse manual actuation commands from the Auxiliary Panel enter through a safety-grade panel. This signal path bypasses the Level 1 PLC. The safety-Class 1E manual panel is the PIPO system. Commands from the PIPO (reactor scram, safety injection) are directly hardwired to the output cards of the SPIN.

The Monitoring and Service Interface (MSI) is treated as safety-Class F1B. The interconnection is enabled via a keyswitch in the control room on the safety panel. The key contact is a hardwired digital input analogous to plant contacts inputs to the protection system. The switch status is interpreted as part of the applications software to change the mode of software to maintenance mode and enable communications between the MSI and the computer under service.

3.5 SIZEWELL B (UNITED KINGDOM)[7,8,9]

Sizewell B is a Westinghouse design PWR that began commercial service in 1995 as the first PWR style reactor in Great Britain. The plant is one of the pioneering examples in the world of a highly integrated control room utilizing digital systems for plant protection. It is the first reactor installed with the Westinghouse Integrated Protection System (IPS); a name used to connote that the system operates as an integrated distributed processor system as opposed to operating on a single integrated processor. The traditional segregation of systems along division lines is generally the same as those in Westinghouse's analog I&C system. The difference is that systems are implemented with digital microprocessor technology and utilize digital data links based on the general distributed computing architecture.

The British regulatory approach employs a risk-based safety analysis rather than solely relying on an application of the single failure criterion. The British safety case for Sizewell also introduced the

[*]N4 PWR computerized operating system (France).
[†]N4 PWR general automation system (France).

idea of the fail-safe state in which the failure modes were guaranteed by the design to place the reactor in the safest configuration in the event of a failure. This innovative thinking has moved the Sizewell B design into a unique category with significant differences in the approach compared to other European reactor installations.

One of the requirements that emerged from the risk-based analysis is the need for a thoroughly diverse protection technology to reduce the risk of a common cause failure in requirements or software design from being a path to failure upon demand. To address this concern, the British added a diverse reactor protection and safety actuation system that drew from British gas reactor protection systems. The secondary diverse reactor protection system is based on the Laddic system, which is based on a pulsed magnetic logic structure and was designed for use at the later Magnox reactors and all advanced gas-cooled reactors. Moreover, no communication link is permitted between the primary and secondary protections systems. No other international reactor protection system has adopted the Laddic technology as a diverse protection system, so the remainder of the discussion focuses on the primary protection system. Nevertheless, the complete independence of the primary and secondary systems gives a significant margin of safety for any common failure modes occurring in the communication links of the primary protection system.

The Sizewell B primary protection system utilizes the Westinghouse EAGLE 2000 series control system for safety systems and their second-generation Westinghouse Distributed Processing Family (WDPF-II) system for nonsafety systems. These systems form the basis for similar systems that are currently operational on nine U.S. plants (Sequoyah 1 and 2, Turkey Point 3 and 4, Watts Bar, Zion 1 and 2, Diablo Canyon 1 and 2) as well as the Temelin plant in the Czech Republic. The IPS performs all the automatic functions required for reactor trip and safety features. It also provides the main control room interface for the qualified display of the Regulatory Guide 1.97 (U.K.) equivalent safety variables, plant startup vetoes and interlocks, manual reactor trip, safety features manual system actuations, and manual control of individual safety features components.

The innovation of the Eagle 2000 family of digital components was the introduction of digital communications. The Eagle 21 system, which preceded Eagle 2000, was designed to duplicate the form, fit, and function of analog components. Hence, the components were installed into analog module racks and used the same terminations and cabling of the analog system. The Eagle 2000 introduced the distributed computing architecture based on the modular workstation. The individual workstations communicated via dedicated, high-performance data highways (WestNet). Also, the architecture provided dedicated, high-speed serial data links between workstations to achieve physical and electronic separation required between channels and to achieve a high level of performance in the safety function response times. These communication links are implemented in both copper and fiber optical cabling. Fiber optical cabling satisfies the requirements for electrical isolation and protection from electromagnetic interference between divisions of the protection system (in the British terminology “divisions” are called “guardlines”). The communication system was designed to recognize interrupted transmission and transfer to a predefined fail-safe state. The failure detection and fail-safe concept are important aspects of the Sizewell protection system’s hazard analysis, particularly for environmental events such as cabinet fire, which might have widespread and unpredictable outcomes on different components.

The general arrangement of a division called a guardline is shown in Fig. 3.4. The individual microprocessor racks correspond to the three levels of components in Fig. 3.1. The Integrated Protection Cabinet (IPC) corresponds to the signal input and comparator level. The Integrated Logic Cabinet represents the voter. The plant switchgear corresponds to the component control. The lines between channels are dedicated high-speed data links. The data links communicate between guardlines and external users via optical data links using predefined message format with appropriate diagnostic features.

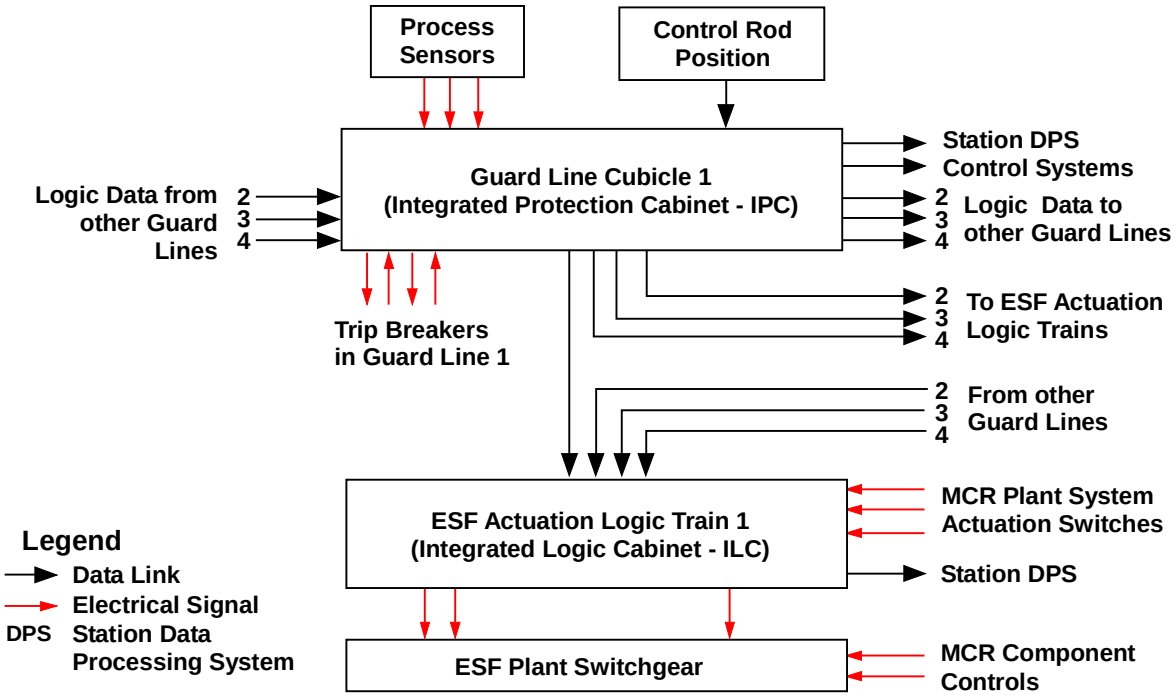

Fig. 3.4. Sizewell B protection system diagram illustrating communications within a division.[10]

The primary protection system, consisting of the reactor trip system and the engineered safeguards, is illustrated approximately in Fig. 3.5. The figure is the best available in the public domain but lacks sufficient detail to illustrate the network connections. The top-level plant data

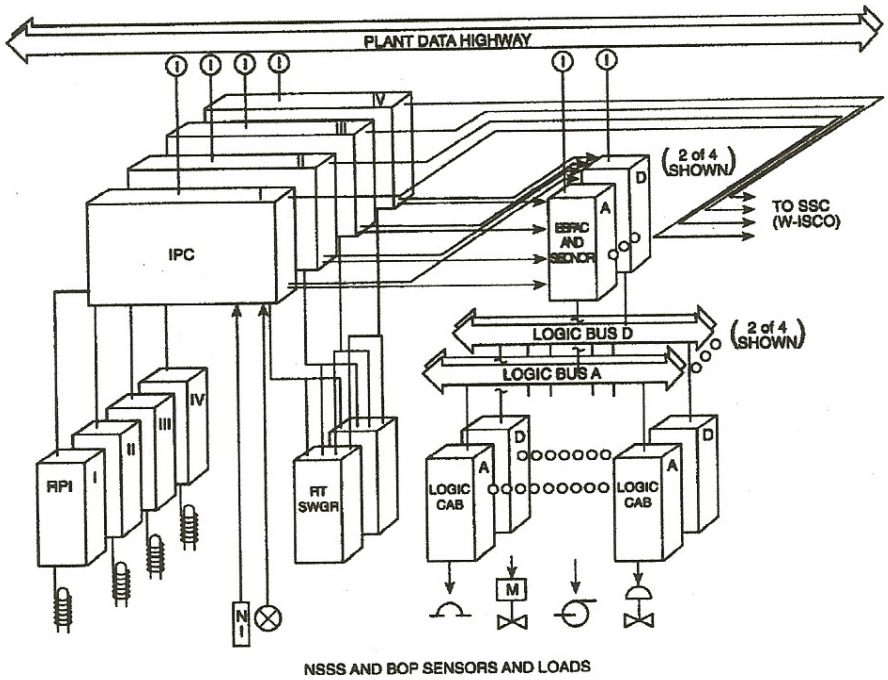

Fig. 3.5. Sizewell B primary protection system.[11] *Source*: G. W. Remley, B. M. Cook, and P. A. Loftus, "Sizewell B Integrated Control and Instrumentation System: A Vision Becomes Reality," IEEE 0-7803-0883-2/93.

highway is the Westinghouse WestNet. All sensor data and protection system settings are available in the main control room through the safety network.

The primary protection system contains an automatic testing and manual self-testing system. Each division is equipped with a complete automatic testing system. The test system has isolated communication links (networked) to each protection system processor to enable all functions to be monitored against stored data during the test process. The test system injects analog test signals and monitors the response from each module connected. Most of the modules can be tested from input through to the output to the system breakers or actuated devices while the system is operational. The automatic tester consists of a computer-controlled subsystem that controls test relays to place channels into test mode. The system varies all signals systematically across their operating ranges and operates the data links. The data links between the processors both control the test and record the results. Test printouts and displays are available in the main control room. When not in test mode, the test computer continuously runs a self-test program and monitors the status of the safety system processors. The test computer is not shown on the figures but roughly corresponds to the arrangement of the generic design in Fig. 3.2.

3.6 DARLINGTON (CANADA)

The Darlington Canadian deuterium-uranium (CANDU) reactors employ two independent, diverse, reactor trip systems referred to as Shut Down System One and Two (SDS1 and SDS2). Each SDS contains three independent trip divisions. Two-out-of-three trip voting logic is employed between the divisions in both SDSs. Final trip voting is performed with relay logic. Each division in SDS1 generates a division trip vote whenever any trip parameter exceeds its set point. SDS2 performs a software vote of each trip parameter in each division. A reactor trip signal is generated if two-out-of-three of the SDS2 trip divisions vote to trip on a particular trip parameter.

Each SDS trip computer also sends plant parameters, alarms, and status information via one-way optical fiber links to a division display and test computer. The display and test computers, in turn, drive two dedicated monitors via optical fiber one-way serial data links to the main control room. Fig. 3.1 shows the testing, control, and display portions of SDS1 and SDS2. Each SDS system also includes a monitoring computer that allows the operator to display system information on demand and to execute system test and input of calibration data. The SDS monitoring computers receive their data via one-way optical-fiber-based serial data links from each division's display and test computers. The SDS monitoring computer is the lowest level common component to the SDS systems. The SDS monitor function includes data consistency checking between the SDS divisions. The SDS monitor computers are connected via one-way, optical-fiber serial links to a plant-level safety system monitoring computer acting primarily as a plant safety-system data historian.

When a system test, calibration, or division bypass is to be performed, the SDSs monitor data transmission links to a division's display, and the test computer and trip computer are enabled. All SDS data transmission is over optical fiber. Each link includes a mechanical interlock mechanism that prevents the SDS monitor computer from being able to transmit data to more than one trip division at once. If any division within an SDS is voting for a trip, the SDS monitor layer computer prevents another division of that SDS from being placed in bypass for testing. The SDS data transmission links are shown as dotted lines in Fig. 3.6. All components of the SDS have to meet stringent qualification standards. Canadian regulators employ a graded safety classification system. While the SDS monitor computers are not within the same safety class as the trip computers, no commands are permitted to be transmitted to the SDS trip computers from nonsafety-grade systems.

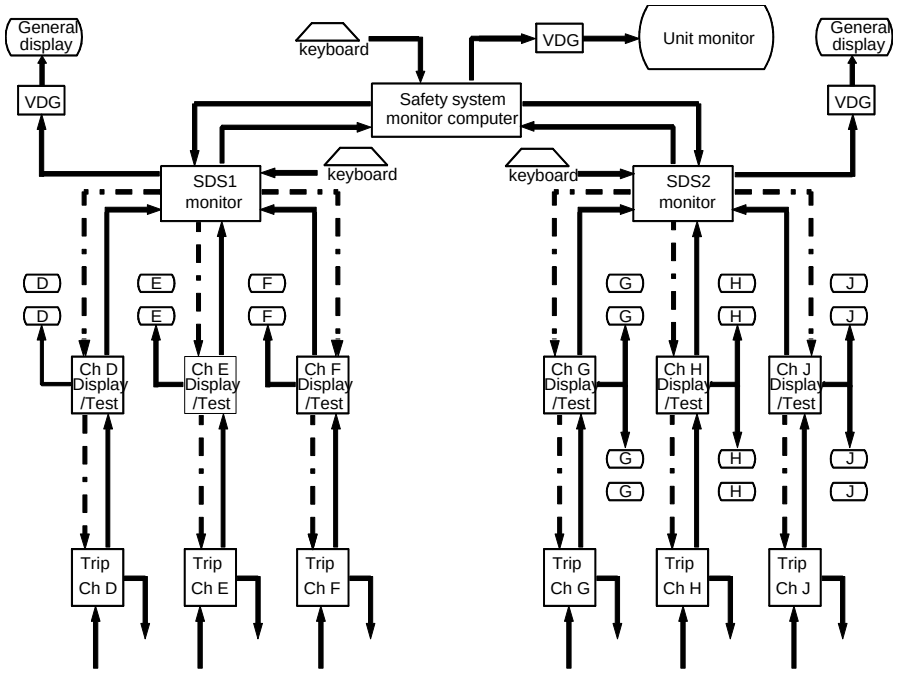

Fig. 3.6. Reactor protection system architecture.

A summary of the parameters of the safety SDSs is provided in Table 3.2.

Table 3.2. Darlington SDS parameters

System	SDS1	SDS2
Reactor protection system	Three divisions	Three divisions
Trip logic	Two-out-of-three division trip relay logic. Division trip vote issued for any trip parameter exceeding set point. Each sensor directly connected to trip computer. Redundant sensors employed for measured parameters	Two-out-of-three software voting for each trip parameter between divisions. Each sensor directly connected to trip computer. Redundant sensors employed for measured parameters
Intradivision communication media	Optical fiber	Optical fiber
Trip data refresh time	~50 ms	65 ms

3.7 LUNGMEN ABWR (TAIWAN)

The digital communication technology being deployed at the Lungmen ABWR will result in fully digital implementations of both the safety and control systems. The communications architecture for the Lungmen nuclear power site was described at the ANS 5th International Topical Meeting on Nuclear Plant Instrumentation Control and Human Machine Interface Technology[12] and the NRC 19th Annual Regulatory Information Conference.[13]

3.7.1 Reactor Protection System Architecture

The Lungmen ABWR has grouped the reactor protection system (RPS) along with the isolation functions into a system referred to as the reactor trip and isolation function (RTIF). Both the acronyms RPS and RTIF are commonly used. All of the RTIF is implemented using GE NUMAC hardware. Principal features of the RPS communications system (illustrated in Fig. 3.7) are as follows:

- The RPS signal communication from sensors to the digital trip module (DTM) is implemented in a nonnetworked topology. Sensors with short response time requirements are directly wired to the DTM, while those with longer response time allowances are connected to remote multiplexing units (RMU), which are then in turn connected to the DTM units.
- The RMU units employ a General Electric (GE) specific fiber distributed data interface (FDDI) protocol for communication with the DTM units.
- The division trip logic is communicated between divisions by means of individual optical fibers between each DTM and trip logic units (TLUs). The voting network does not pass through the main control room.
- RPS bypass is performed using dedicated controls (not shown in the figure), connected via optical fiber, on the main control console.
- The TLUs from each division are directly connected, via output logic units (OLUs), to trip load drivers (current interrupters), which are configured in a redundant two out of four arrangement.
- The main control room also has a manual scram function that is directly wired to both control rod current interrupters. Actuation of either control rod current interrupter independently leads to rod insertion (one-out-of-two configuration).
- The RPS communicates to both the plant data network and triple modular redundant control systems using RS-485 protocol buffered by separate safety-grade, one-way protocol interchange gateways. The RS-485 protocol is two-way in that it supports network handshaking. Consequently, both ends of the RS-485 links are safety-grade. The downstream protocol interchange gateways serve to prevent information from the nonsafety system from propagating to the safety system.
- Each RPS division provides its status information to the engineered safety feature (ESF) system network using the RS-485 protocol buffered by a protocol interchange module with qualified isolation. Apart from the protocol handshaking, the data link is one-way even though both networks are safety-grade.
- Each RTIF division has direct connection to the triple modular redundant controllers to provide feedwater control commands.

Arrowheads in Fig. 3.7 indicate direction of information flow. Dashed lines indicate optical fiber communication paths. Blue components are nonsafety, and black components are safety grade.

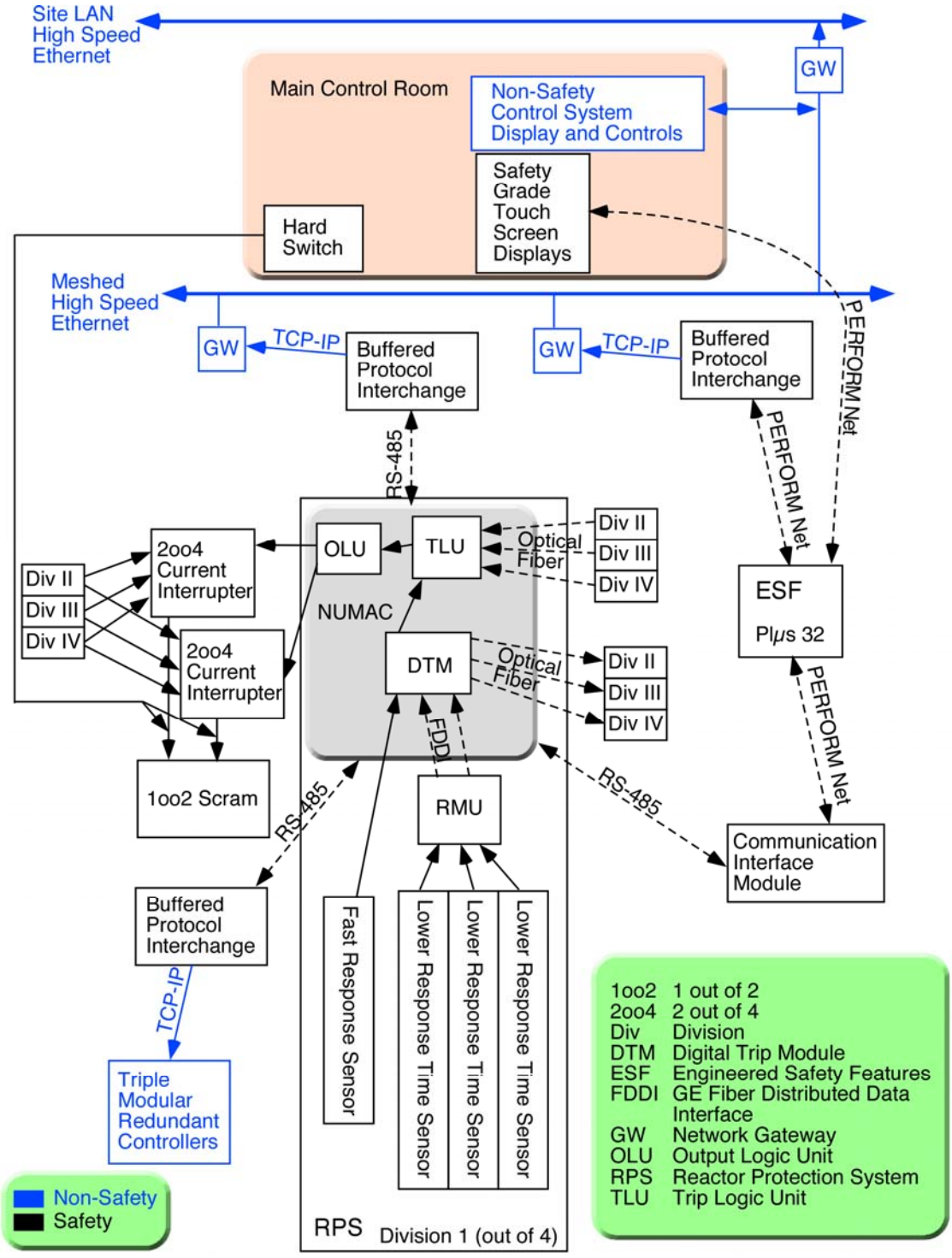

Fig. 3.7. Lungmen reactor protection system communications paths and protocols.

3.7.2 Engineered Safety System Architecture

The Lungmen ESF system is implemented using the Programmable Logic Microprocessor System: 32 bit (PlμS 32) from DRS. The ESF system network topology is a dual-redundant fiber optic ring with deterministic timing referred to as the essential multiplexing system (EMS).

Fig. 3.8 shows the EMS network topology in block diagram fashion. The EMS network is configured as five independent serial ring networks (four rings supporting the ESF and one allowing either Lungmen unit one or two to access a spare swing set of emergency diesel generators). Each ESF system is connected to two of these separate optical fiber ring networks. Each block exterior line color in Fig. 3.8 corresponds to the ring in a division with which the unit is connected. Variegated color lines indicate that the unit is connected to both rings within a division.

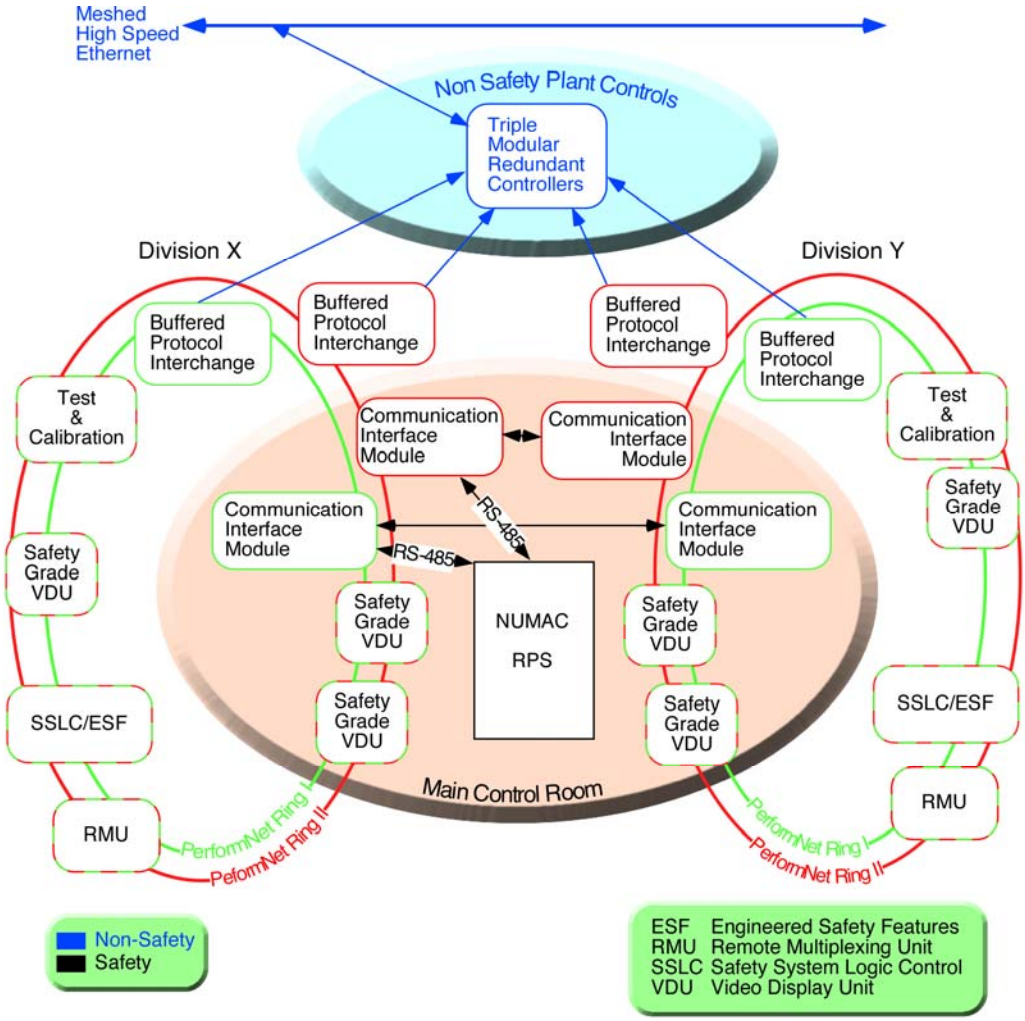

Fig. 3.8. Lungmen essential multiplexing system network topology.

The EMS network is arranged into two divisions of fiber optic rings. Each ring communicates with two ESF divisions; one division of rings communicates directly with two ESF divisions, and another division of rings communicates directly with the other two ESF divisions. The video display units (VDU) for the ESF system are directly connected to the EMS network. The RPS is connected to the EMS via two optical fibers, each of which connects serially to two communications interface modules, one on each of the EMS network sets. The EMS rings both use distributed input, control, and output modules for data acquisition, logic, and plant controls (the network is logically bidirectional). Message flow around each EMS ring is physically—around each ring (dual counter-rotating ring topology within each division). The VDUs provide data display and a command interface in the control rooms. Each safety-grade, touch-screen VDU is dedicated to communication with a particular EMS division. While the safety-grade VDUs do display the RPS status, no RPS

command interface is provided via the touch-screen VDUs. Safety commands can only be performed from safety-rated equipment. However, safety information is also displayed on nonsafety-related displays through one-way buffered gateways.

The EMS network is implemented as a PERFORM (performance-enhanced redundant fiber optic replicated memory network). This is a proprietary network topology of the DRS PlµS 32 system. Each node on a ring set has identical replicated memory (512 K bytes for Lungmen). The memory is segmented into 4-K byte blocks with each block assigned to a particular node. Each node can only write to its own 4-K byte address space. However, each node can read from the entire address space. The network serves to replicate the contents of each node's memory to the other nodes on the ring set. Each node has two separate interface modules, each accessing one of the rings of the set. Each node thus contains a complete set of the ring's 512-K byte data set.

3.8 TEMELIN (CZECH REPUBLIC)[14,15]

The Temelin Nuclear Power Plant is a Russian-designed VVER 1000 PWR plant. Following the breakup of Eastern bloc countries and the Chernobyl accident, a concerted effort was directed toward upgrading the level of safety of the Russian-made plants in Eastern Europe to western licensing standards. The VVER 1000 plant, being the most recent of the Russian-designed plants, was considered safe in all respects except instrumentation and controls.

The upgrade of the Temelin plant was not a replacement of the Russian protection system, but an addition to the Russian control and monitoring system of a completely automated digital protection and control system. The Czech Republic chose the Central Electricity Generating Board (CEGB), now British Energy, owner and operator of the Sizewell B plant, to be a consultant on the project and assist in preparing a specification of the digital upgrade. The protection system design ultimately chosen was the Westinghouse Integrated Protection System (IPS) concept using Westinghouse Eagle hardware like the Sizewell B plant. While Sizewell B and Temelin are both designed and implemented based on the Westinghouse IPS concept and Eagle hardware, some significant differences in hardware and scope of the systems should be noted. First, the Czech design is closer to the IPS standard design because manual control of the safety components is not accomplished with a separate system as required in the United Kingdom but is part of the primary protection system. Second, the Temelin design was only able to implement a triply redundant architecture at the division level. The VVER plants were originally designed with triple and dual redundant sensors. Because the old Russian system was retained, it was not possible to upgrade to quadruple instrumentation. The plant level network for Temelin was upgraded with the introduction of a standard fiber distributed data interface (FDDI) for the nonsafety plant level data highway in place of the WDPF network used on Sizewell. This boosted the transmission rate to 100 million bits per second compared to the 2 million bits per second for the WDPF system. This significantly eased the design problems for display and control systems. Additionally, the Eagle processor modules were upgraded from Intel 80286 and 80386 processor to Intel 80486 processors. This last change was implemented at the hardware level without recompiling the system software.

Interdivision communications for voting is provided by optical data links that are similar to Sizewell. The reactor protection and ESFAC outputs are provided to the data highways through optically isolated gateways for use in the plant control systems and plant information system. In the communications links, all components except the data highways and the gateways between the data highways and the safety system data links are 1E qualified components. The gateways, interestingly, are not 1E. Individual component level control outputs and classical equipment status indications are proved through the Eagle internal safety networks to the automatic control system and plant information system.

The protection system software contains internal diagnostics for module and communications faults. In addition, a mobile tester is provided that automates the surveillance procedures. Details about the connection and channel bypass for testing are not available in current resources.

A function-level diagram of the protection system is given in Fig. 3.9.

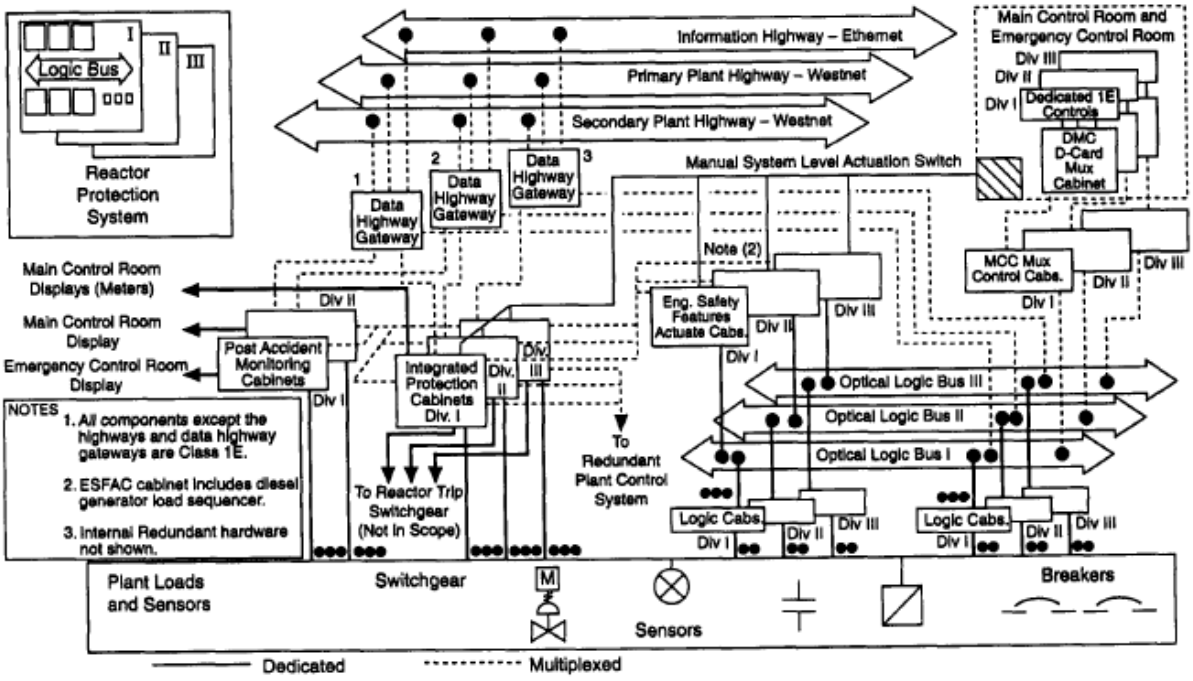

Fig. 3.9. Temelin reactor protection system.[15]

3.9 DUKOVANY (CZECH REPUBLIC)[16]

The Dukovany Nuclear Power Plant Unit 3 is a pressurized-water plant of the VVER/V213 design located in Trebic in the Czech Republic. Its control and protection systems were upgraded in 2002 to bring the protection systems up to international licensing standards. The upgrade was constructed using SPINLINE 3 provided by Data Systems and Solutions (DS&S).

The architecture of the system consists of three divisions with two-out-of-three voting. NERVIA is the standard network protocol for SPINLINE 3 for both safety and nonsafety applications. There are three NERVIA networks, one per division. The NERVIA 1E network is a 10-megabit/second, deterministic, broadcast-type, token ring network. A broadcast protocol means that any message sent by one unit is received by all. A network cycle circulates a token to each network station in a predefined order. A station is allowed to transmit its data on the network only when it owns the token and within a specified time window. Data are transmitted in blocks and are validated using a cyclic redundancy check (CRC). The network and the modules connected to it operate asynchronously. Operation of any module is not dependent on the operation of the network or vice versa. A stall of one component, either network or module, does not cause another system to also stall. All three NERVIA networks are connected to the plant computer through a gateway to the plant information Ethernet network.

3.10 OLKILUOTO-3 (FINLAND)

The European Pressurized Reactor (EPR) is an advanced evolutionary PWR designed by FANP, an AREVA and Siemens company. It is currently under construction in Finland as Unit 3 of the Olkiluoto plant [(OL)-3]. Three variants of the EPR design are either under construction [e.g., OL-3 and Flamanville (FL)-3 in France] or undergoing design certification [i.e., the U.S. EPR]. This design

overview refers to the Olkiluoto-3 I&C systems. The design differences among the three EPR I&C variants are outlined in Table 3.3.

Table 3.3. Differences in I&C among the different EPR designs*

System	OL-3	FL-3	U.S.
Protection System (PS)	TXS	TXS	TXS
Safety Automation System (SAS)	TXP	TXP	TXS
Reactor Control, Surveillance, and Limitation (RCSL) System	TXS	TXS	TXS
Process Automation System (PAS)	TXP	TXP	TXP
Priority Actuation and Control (PAC) System	TXS (priority modules)	Switchgear cabinets	TXS (priority modules)
Safety Information and Control System (SICS)	Mostly conventional I&C, limited QDS	Mostly QDS, limited conventional I&C	Mostly QDS, limited conventional I&C
Process Information and Control System (PICS)	TXP	TXP	TXP
Severe Accidents Automation System (SAAS)	TXS	See note 1	TXS
Diverse protection functions	TXP/HBS	TXP	TXP

Note 1: No information available
Legend:
PS—Protection System; SAS—Safety Automation System; RCSL—Reactor Control, Surveillance, and Limitation system; PAS—Process Automation System; PACS—Priority Actuation and Control System; SICS- Safety Information and Control System; PICS—Process Information and Control System; SAAS—Severe Accident Automation System; TXS—TELEPERM XS; TXP—TELEPERM XP; QDS—Qualified Display System; HBS—Hardwired Backup System.

3.10.1 OL-3 I&C Overall Architecture

The EPR main I&C systems and subsystems are listed in the first column of Table 3.3 and illustrated in Fig. 3.10. All functions necessary to achieve a safe shutdown state are either automatically generated in the SAS or manually initiated and processed by the PICS and SAS.[17]

PAC modules monitor and control both safety-related and nonsafety-related actuators. Each actuator being controlled requires a separate PAC module (Fig. 3.11). All commands to these actuators are routed through the PAC. PAC modules receive actuation requests, and process them according to the command priorities encoded into the PAC module logic circuitry to generate command outputs that are routed to their actuator. The PAC input signals can include status and health monitors for the actuator it controls. Depending on the current operational situation, contradictory commands may be given by different I&C subsystems to particular actuators. Consequently, prioritization rules have been established, and encoded into each PAC module, to

*Personal communication with Mark Burzynski, AREVA.

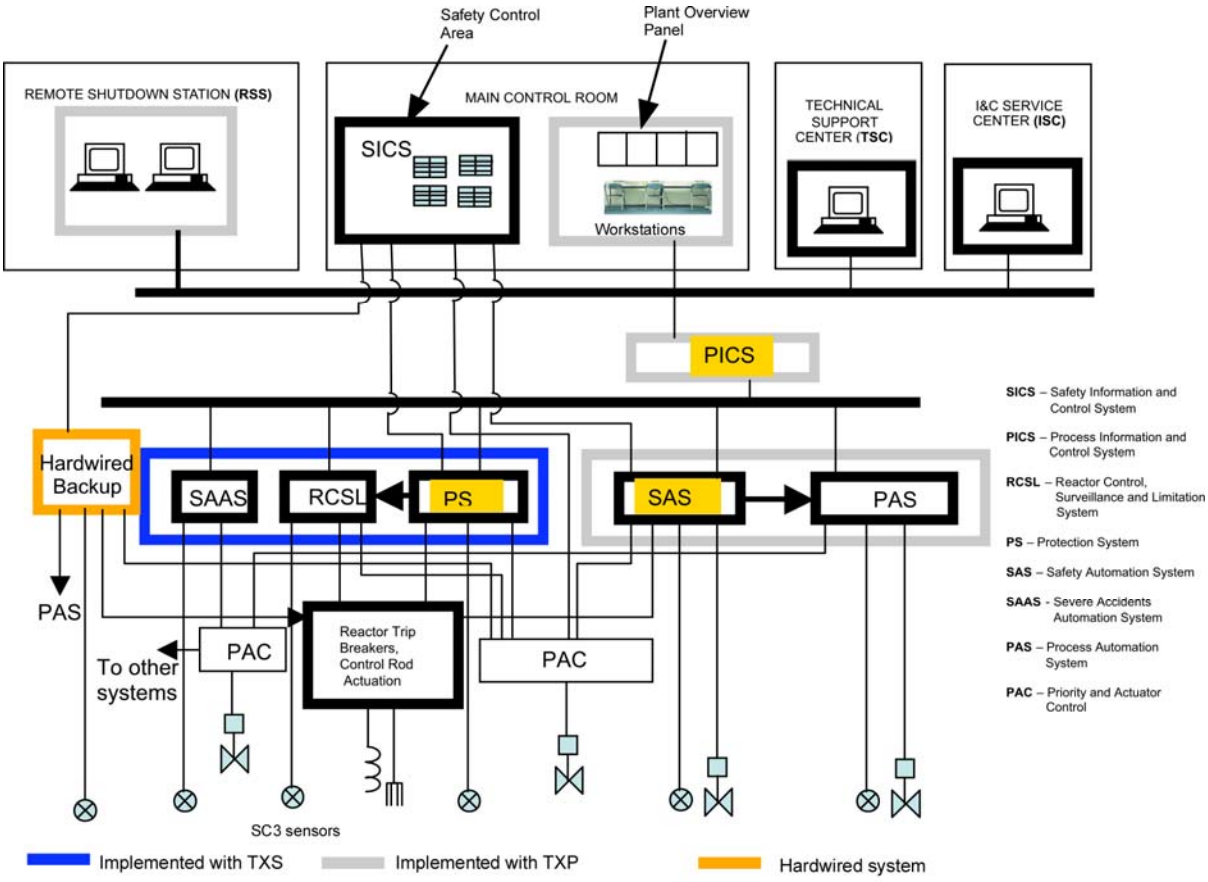

Fig. 3.10. Olkiluoto 3 I&C architecture. (*Source:* J. Hyvarinen, STUK)

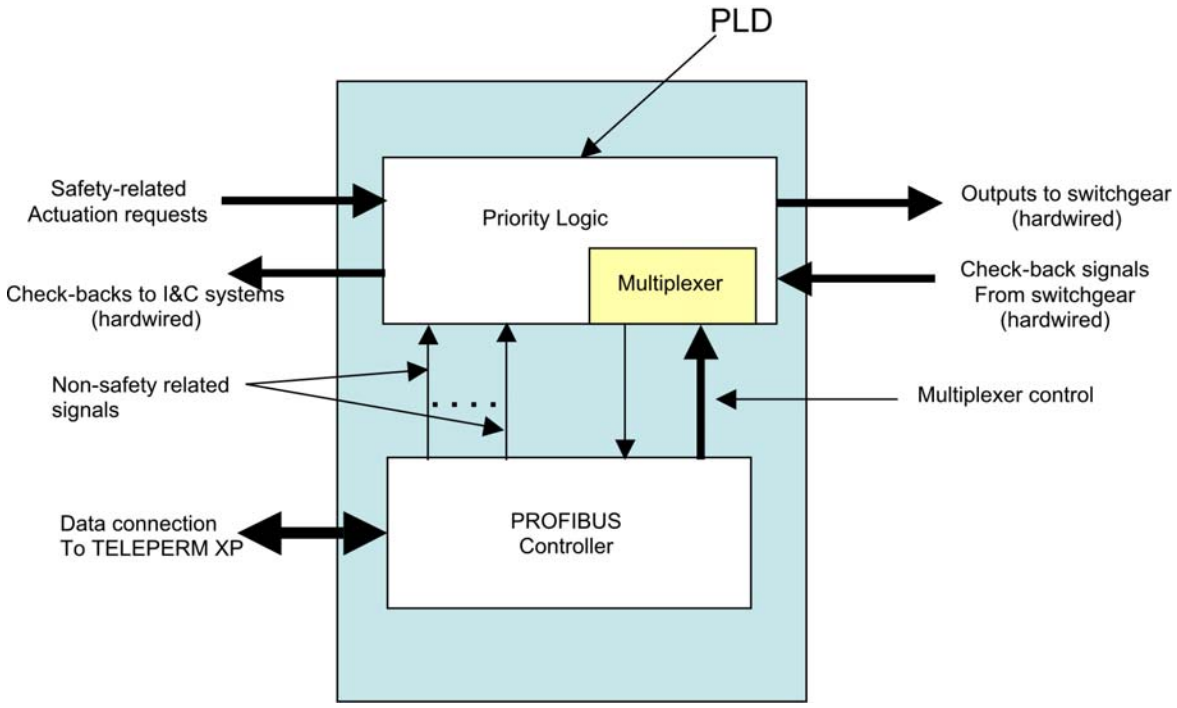

Fig. 3.11. Block diagram of Olkiluoto 3 priority and actuation module.

resolve any conflicting commands such that the unit will always respond to the highest priority command. Each PAC module has two major components as shown in Fig. 3.4. The first is a programmable logic device (PLD) that consists of interconnected logic gate arrays. The second is an application-specific integrated circuit (ASIC) PROFIBUS controller, which provides the communication interface to the TELEPERM XS (TXS) of the PS, RCSL, or the SAAS, or the TELEPERM XP (TXP) of the SAS.

The RCSL system provides automatic, manual, and monitoring functions to control and limit the main reactor and nuclear steam supply system parameters if they deviate from desired operational values before the parameters reach trip set points. The RCSL system is intended to reduce reactor trips and PS challenges. For example, the RCSL is designed to take actions such as runback of power if the plant operational parameters exceed their operational boundaries to prevent challenging the PS.

The SAS controls certain safety-related support systems, such as component cooling water system (CCWS) and ventilation. The PAS controls nonsafety-related systems, and also contains some backup functions for reactor trip and actuation of ESF that are implemented using diverse hardware and software from the primary reactor trip and ESF actuation systems. The PS is implemented with the TXS platform. The TXS system architecture basic building blocks can be grouped into the following 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 and programmable, read-only memory for storing program code; and electrically erasable and 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 that was developed, by Siemens, specifically for the TXS system. 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 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 that use qualified software modules from a function block library to construct a specific application.

Important software features of the TXS include the following:

- Strictly cyclic processing of application software. That is, the system processes data asynchronously, i.e. there is no real time clock with which redundant processors synchronize.
- No dynamic memory allocation. Each variable in the application program has a permanent dedicated place in memory, so that memory conflicts due to dynamic memory allocation are eliminated.
- No process-driven interrupts.

The SAS is a digital I&C system devoted to automatic control, manual control, and measuring and monitoring functions needed to bring the plant to a safe shutdown state. Its functions include

- Post-accident automatic and manual control as well as the monitoring functions needed to bring the plant to the safe shutdown state; and
- Automatic initiation of I&C functions to prevent spurious actuations that could result in design basis accidents.

The SAS receives process data from plant instrumentation and switchgear, sends actuation signals either directly or via the PAC, and sends monitoring signals to the SICS and PICS.

Communication

Each I&C system manages its own internal exchanges (including data exchange between divisions) without using external resources. Data exchange between the different I&C systems is performed primarily through standard exchange units connected to the corresponding system networks.[*,18] Note that OL-3 uses two-way communication between PICS and PS/SAS.

Mode of Sensor Signal Transmission and Shared Sensor Implementation

Most sensors use 4- to 20-ma (or in some cases 0- to 5-V) analog transmission. There is no sharing of sensors between functionally diverse subsystems (i.e., between sensors on subsystem A and sensors on subsystem B).[19] However, partial trip data is shared between divisions for voting. Measured sensor signals are also shared for the purpose of signal validation.

Hardwired Backup Systems

Olkiluoto-3 design provides an automatic hardwired backup system (HBS). The HBS contains a small subset of the protection system functions. They include automatic actions needed to cope with certain design basis events. The HBS uses field programmable gate array (FPGA) technology. The FPGA is not programmable while installed, and it is considered sufficiently diverse from the other major platforms. In addition to the automatic HBS, a manual HBS is also provided.

I&C Design Features to Reduce the Probability of Unintended Behaviors and/or Latent Faults in the Safety System(s)

Features include

- Deterministic processing,
- Asynchronous operation of each computer—extensive self-monitoring,
- Signal validation techniques,
- Voting techniques,
- Inherent and engineered fault accommodation techniques,
- Software life cycle including V&V,
- Operating experience with standard library of application software function locks, and
- Communication independence measures.

3.10.2 Digital I&C Issues and How they are Addressed in the EPR

Fig. 3.12 shows the MSI (not shown in Fig. 3.10) that forms the boundary and interface between the safety system and the safety panel in the control room. It also forms a safety-related logical barrier between the rest of the safety system and the nonsafety interfaces. Its safety classification is 1E (Finnish Class SC-2) system. The MSI computers (Fig. 3.12) is designed to ensure that only predefined messages are transferred between the safety system and nonsafety-related displays; the MSI is not responsible for plant control functions.

Communication via the maintenance panel (Service Unit) to a safety channel can be performed only after that channel has been turned off via a keyswitch. For OL-3, the TXS equipment (i.e., the four divisions of the protection system) are located in the four safeguards buildings.[†] The processor

[*] This information primarily pertains to the U.S. EPR. While specific information on communication methodology for the OL-3 could not be obtained, the I&C architecture and communication methods for the OL-3 and US EPR are similar.

†This is also true for the U.S. EPR.

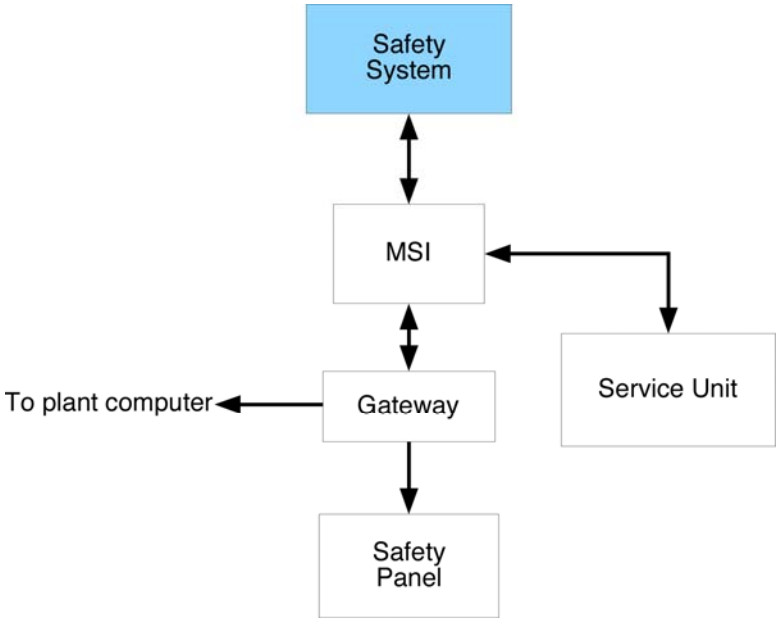

Fig. 3.12. The MSI forms a logical boundary between the rest of the safety system and the nonsafety interfaces.

key switches are located in the equipment cabinets.* Maintenance data is written to the MSI in a separate area of memory.

The MSI is in continuous communication with the safety divisions to receive status and diagnostic information. This information includes continuous checks for sensor deviation (the Auto Channel Check feature). Many precautions are taken to prevent access through the MSI from affecting the safety function. These precautions include strict access control features and predefined connection/messaging protocols. In addition, the MSI confirms the identity and bypass status of a safety division to ensure that maintenance access is enabled only for one division at the same time and when that division is in bypass. However, once access to a safety division through the MSI is granted, it is possible to alter the parameters of the safety application's logic blocks. The MSI also provides a connection to plant computers, but it is a one-way uplink.

The SICS consists of a small inventory of conventional (continuously visible) human-machine interface (HMI) and a series of qualified displays (QDS). The QDS are safety-related and are therefore required to be qualified to Finnish Class SC-2 (U.S. Class 1E) standards. Nonsafety-related information can be displayed on the SICS. Any nonsafety data displayed on SICS is processed by a safety-related Class 1E computer before being sent to the SICS display; therefore, there is no co-mingling of safety and nonsafety software on the SICS display system.

REFERENCES

1. The Institute of Electrical and Electronics Engineers, IEEE Std. 603-1998, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," IEEE, New York (1998).

2. International Atomic Energy Agency, "Safety of Nuclear Power Plants: Design, Safety Standards," Series No. NS-R-1, IAEA, Vienna (2000).

3. International Atomic Energy Agency, "Protection System and Related Features in Nuclear Power Plants: A Safety Guide," Safety Series No. 50-SG-D3, IAEA, Vienna (1984).

*The TXS equipment cabinets are located in the control room for Oconee.

4. International Atomic Energy Agency, "Instrumentation and Control Systems Important to Safety in Nuclear Power Plants," Safety Series No. NS-G-1.3, IAEA, Vienna (2002).

5. International Electrotechnical Commission, IEC 1226, "Nuclear Power Plants—Instrumentation & Control Systems Important for Safety-Classification," 1993.

6. International Atomic Energy Agency, "Specification of Requirements for Upgrades Using Digital Instrument and Control Systems," IAEA-TECDOC-1066, IAEA, Vienna (1999).

7. *Advanced Reactor Licensing: Experience with Digital I&C Technology in Evolutionary Plants*, NUREG/CR-6842, ORNL/TM-2004/74, Oak Ridge National Laboratory, April 2004.

8. G. W. Remley, B. M. Cook, and P. A. Loftus, "Sizewell B Integrated Control and Instrumentation System: A Vision Becomes Reality," IEEE.

9. G. B. Moutrey and G. Remley, "Sizewell B power station primary protection system design application overview: Electrical and Control Aspects of the Sizewell B PWR," International Conference on 14–15 September 1992, p. 221–231.

10. Ibid.

11. Remley, Cook, op. cit.

12. Chia-Kuang Lee, *The Network Architecture and Site Test of DCIS in Lungmen Nuclear Power Station*, 5th International Topical Meeting on Nuclear Plant Instrumentation Control and Human Machine Interface Technology (NPIC & HMIT 2006), November 12–16, 2006, Albuquerque, New Mexico U.S.A., pp. 747–54.

13. Chang-Fu Chuang and Yi-Bin Chen, presentation at *Regulatory Overview of Digital I&C in Taiwan Lungmen Project*, NRC 19th Annual Regulatory Information Conference, March 13–15, 2007, Rockville, Maryland.

14. *Advanced Reactor Licensing: Experience with Digital I&C Technology in Evolutionary Plants*, NUREG/CR-6842, ORNL/TM-2004/74, Oak Ridge National Laboratory, April 2004.

15. W. C. Gangloff and C. L. Werner, "I&C Modernization for VVER Reactors," *IEEE Transactions on Nuclear Science* **40**(4), 819–825 (August 1993).

16. J.-P. Burel, F. Dalik, K. Wagner, Miroslav RIS, and J.-P. Mauduit, *Modernization of I&C systems for the ANP Dukovany by the use of computer-based equipment*, NEA/CSNI/R(2002)1/Vol. 2.

17. J. Hyvarinen, *OL3 I&C Review Status,* ASN/IRSN-NRC-STUK Mtg., March 22, 2007.

18. *EPR Design Description*, Framatome ANP, Inc., August 2005.

19. Ibid.

4. CONSENSUS PRACTICES

4.1 REVIEW OF STANDARDS AND GUIDES

This section examines selected standards and guidelines concerning a variety of aspects of digital communications for I&C. The intention in this section is not to compare or evaluate these standards, but to collect from them the accepted practices for digital safety system communication. Note that an older comparison of IEC and IEEE standards relevant to digital communication is found in Ref. 1.

4.1.1 IEEE 603-1998 and IEEE 7-4.3.2-2003

IEEE 603, "Standard Criteria for Safety Systems for Nuclear Power Generating Stations," broadly addresses safety systems. It refers to IEEE 7-4.3.2 when discussing digital computer issues. IEEE 7-4.3.2-2003, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations," discusses independence between safety channels and between safety and nonsafety channels in Sect. 5.6.

The issue of importance is that data communications between safety channels or between safety and nonsafety channels shall not inhibit performance of the safety function. The standard recommends erecting barriers as an alternative to requiring all communications components that interact with the safety system be safety grade. Annex E of the standard suggests broadcast (one way) and buffered solutions to prevent prohibited interactions between the computer processor performing safety functions and other devices. The general configuration for the buffered solution of Annex E is depicted in Fig. 4.1. A more detailed implementation of the buffering scheme is shown in Fig. 4.2.

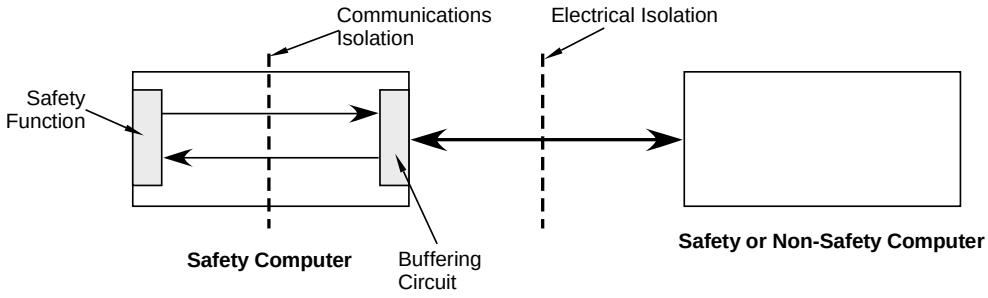

Fig. 4.1. Concept of communication buffering from IEEE 7-4.3.2-2003 Annex E.

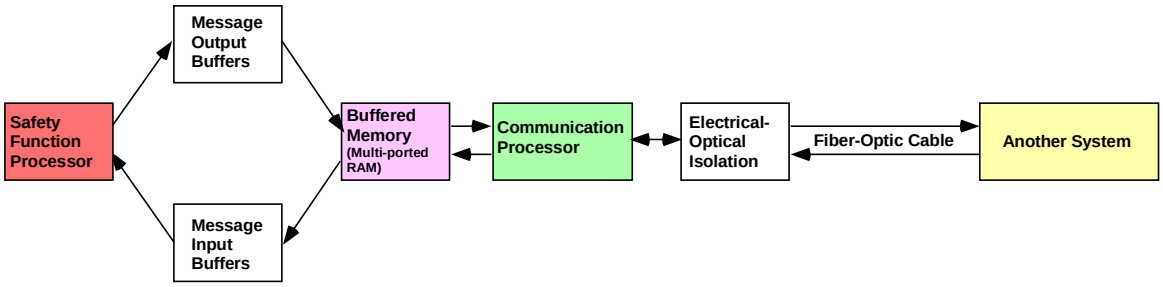

Fig. 4.2. Possible implementation of communication buffering using multiported memory.

The key feature of buffered communication is that loading of the safety function process is unaffected by communications tasks. One of the key concepts in the buffering scheme is use of a separate communications processor with structured access to (dual-port) memory shared with the safety function processor. A revision of IEEE 7-4.3.2 is planned to more fully describe possible approaches.

4.1.2 IEC 61500

The IEC 61500 standard,[2] "Nuclear Power Plants—Instrumentation and Control Systems Important to Safety—Functional Requirements for Multiplexed Data Transmission," 1996, is a set of requirements that is applicable to data transmission by multiplexers or Fieldbus systems using a shared bus. It lists broad requirements for the following categories:

- Function, performance, safety class, and network topology;
- Communications protocols;
- Communications media;
- Reliability and independence;
- Operation and maintenance; and
- Qualification.

Security requirements are deferred to other standards groups.

The standard's requirements were written to be broadly applicable. It is useful as a yardstick for assessing a custom-designed communications network; however, there are now standards for the popular Fieldbus networks.

The major recommendations are

- Isolation of safety systems,
- Reliable and timely delivery of safety commands and data despite the communications medium sharing,
- Network topology that reflects segregation of safety classes and redundancy for fault tolerance,
- Equipment separation through electrical isolation and physical separation,
- Equipment function separation through send and receive on separate hardware,
- Communications software separated from data processing software,
- Communications are from higher to same or lower safety classes (simplex),
- Diversity,
- Self-supervision (fault monitoring),
- Reconfiguration and isolation upon component fault (desirable function),
- Fault notification to served equipment including reactor operator,
- Signal validity markers passed with data,
- Testability during operation,
- Maintainability through diagnostic and performance testing facilities, and
- Plug-in replacement modules.

The complexity of a safety system's design is always a point of concern. Complications can arise through functions that depend on past device states (information) or time-dependent exchanges between devices (updating shared signal values). A complicating design issue is bursts of data allowed to record a sequence of events, which also requires an accurate time stamp. The standard notes the practical necessity of such communications—that this must be carefully engineered to avoid network disruption. It also states that precise time synchronization must be a network-wide function, suggesting that this requires communication among all devices/networks involved. Another complicating issue is communicating warnings about communication errors. This implies a display or

logging system to receive such errors but also suggests reporting to “equipment the network serves.” Both of these add complexity to the system.

4.1.3 IEC 61508 and IEC 61513

IEC 61508[3] is a generic process standard for the development of safety-related systems. Its approach is to specify rigorous development practices to increase the probability that the resulting system is safe. IEC 61513[4] is the specialization of 61508 for the nuclear industry. IEC 61513 carries forward the general safety system design guidelines stated in 61500 and adds process guidance for the life cycle of the system—requirements, planning, qualification, integration, operation, and maintenance.

IEC 61513 provides high-level requirements for the safety system. The following section from 61513 on the data communications is typical.

> 5.3.1.3 Data communication
> Data communication between systems making up the I&C architecture includes all the links provided to transmit one or more signals or messages over one or more paths using different multiplexing techniques.
> a) Communication links shall be capable of meeting the overall performance requirements specifications (see 5.2) under all plant demand conditions.
> b) Communication links architecture and technology shall ensure that the independence requirements between systems are met. In addition to physical separation and electrical isolation, the design should include provisions to ensure that problems with communication links do not impair processing modules.
> c) Communication links shall include provision for checking the operation of the communication equipment and the integrity of transmitted data.
> d) Redundancy of the communication links should be provided to accommodate failures.
> e) Communication links shall be designed in such a way that data communication and operation of the higher safety category function cannot be jeopardized by data communication with lower classified systems. For example, tests in operation shall not jeopardize the highest category function.

IEC 61508 states that low complexity systems are not subject to the standard. A low complexity safety-related system is defined in Sect. 3.4.4 of IEC 61508-4 as a safety-related system in which the failure modes of each individual component are well defined and the behavior of the system under fault conditions can be completely determined. This categorization is intended to include such simple devices as limit switches, but there is no restriction that would eliminate, for example, an FPGA (simple electronics) running a formally verified program.

The approach taken by IEC 61508 and its application-specific derivatives has been criticized as being too generic and focused on the development process rather than the final product.[5]

4.1.4 IEC 61784-3

Fieldbus technology is now considered well proven in some application areas. Much more has been done in machinery applications than the process industry. Machinery applications, as opposed to process applications, are more concerned with discrete value signals such as relay positions, which are reported by the instrument when the value changes. Process applications are more concerned with reporting continuous value signals such as pressure. While there are differences, the working assumption is that the process industry will be able to use a nearly identical Fieldbus technology. The 61784 standards[6,7] address extensions to the Fieldbus technologies described in IEC 61158, in a way

compatible with IEC 61508. These extensions are a standardized means of supporting real-time, safety-related, and security-related applications. IEC 61784-3 deals with the following Fieldbus technologies:

1. FOUNDATION® Fieldbus,
2. ControlNet™,
3. PROFIBUS,
4. P-NET®,
5. WorldFIP®,
6. INTERBUS®, and
7. SwiftNet.

These technologies define a subset of the OSI network layers: physical (1), data link (2), and application (7). Specific safety implementations are presented for several technologies in IEC 61784-3.

4.1.4.1 Hard real-time response

The standard addresses hard real-time requirements by specifying the safety-function response time:

> The safety function response time is the worst case elapsed time following an actuation of a safety sensor (e.g. switch, pressure transmitter, light curtain) connected to a Fieldbus, before the corresponding safe state of its safety actuator(s) (e.g. relay, valve, drive) is achieved in the presence of errors or failures in the safety function channel.

All components must be serially counted in the response time, as shown in Fig. 4.3. Besides the sensor and surrounding process, the most variable response time is found in the transmission components. Noise and error correction functions have a stochastic element even in a simple two-node implementation.

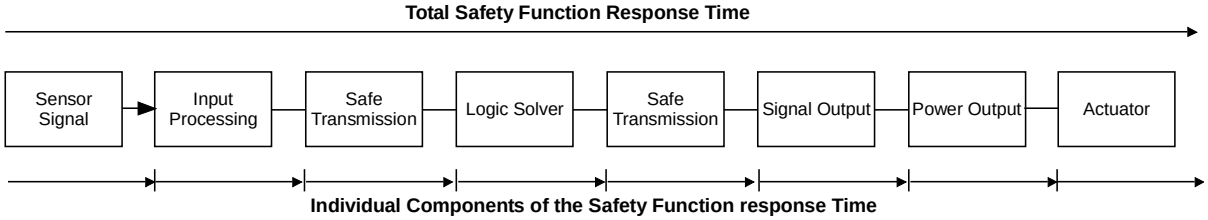

Fig. 4.3. Example of safety-function response time components.

There are two types of responses in the presence of an error. First, the conservative response is for the system to recognize the communications error and execute the safety function. This response handles hard failures. It can require that all of the control nodes on the network know the appropriate actions to produce a safe state and can execute the actions in the event of a communications failure. Second, the system can correct the communications error in time to perform the safety response in the event that it is necessary. This latter response handles transient failures; however, it puts tight constraints on the timing of the system in the face of errors.

The technologies described in the standard are not restricted to cyclic bus operation: acyclic (event-driven) messaging can occur. A technology (e.g., PROFIBUS™) might restrict acyclic message use to modes without real-time safety functions (i.e., maintenance, bypass, configuration, parameterization, diagnosis, installation, etc.).

4.1.4.2 Safety-related layer

A major component of the safety concept presented is the Safety Communication Layer (SCL) (Fig. 4.4). This is a communications layer in the sense of the standard OSI model, present on the safety-related equipment on the network. Its function is to ensure that the system, as a whole, maintains safety regardless of any communications errors that occur. It covers possible transmission faults, remedial measures, and considerations affecting data integrity.

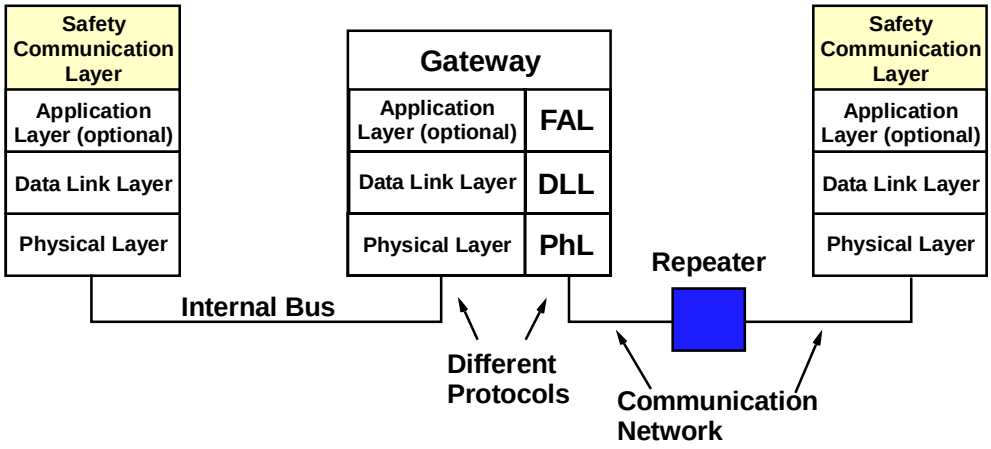

Fig. 4.4. Three-level layer model with SCL applied to a safety system network. This figure is similar to Fig. 2.3 except with the SCL added.

For example, a safety layer can implement an additional message CRC to lower the probability of accepting a corrupted message to the level required for the safety function. Table 4.1 of the standard lists the types of communications errors and the safety measures that effectively mitigate them.

4.1.4.3 Safety measures

The safety measures outlined in Sect. 5.4 of IEC 61784-3 can be related to the set of possible errors, defined in Sect. 5.3. This relationship is shown in Table 4.1. Each safety measure can provide protection against one or more errors in the transmission. The evaluation process is to demonstrate that there are one or more corresponding safety measures for the defined possible errors in accordance with Table 4.1.

The SCL is designed to achieve a reliability of detecting and handling such errors according to the Safety Integrity Level (SIL) that has been determined for the application. (While not necessary from a strict evaluation, since no active nuclear plant performs a SIL 4 function, reactor safety systems are typically designed and developed as SIL 4 systems.)

Table 4.1. Overview of measure effectiveness on possible communication errors (from IEC 61784-3)

Communications errors	Safety measures							
	Sequence number	**Time stamp**	**Time expectation**	**Connection authentication**	**Feedback message**	**Data integrity assurance**	**Redundancy with cross checking**	**Different data integrity assurance systems**
Corruption					X	X	Only for serial bus[d]	
Unintended repetition	X	X					X	
Incorrect sequence	X	X					X	
Loss	X				X		X	
Unacceptable delay		X	X[c]					
Insertion	X			X[a,b]	X[a]		X	
Masquerade				X[a]	X[a]			X
Addressing				X				

Source: Adapted from IEC 62280-2 and GS-ET-26; "Grundsatz für die Prüfung und Zertifizierung von Bussystemen für die Übertragung sicherheitsrelevanter Nachrichten," May 2002. HVBG, Gustav-Heinemann-Ufer 130, D-50968 Köln ("Principles for Test and Certification of Bus Systems for Safety relevant Communication").

[a]Depends on the application.

[b]Only for sender identification. Detects only insertion of an invalid source.

[c]Required in all cases.

[d]This measure is only comparable with a high-quality data assurance mechanism if a calculation can show that the residual error rate reaches the values required in IEC 61784-3 Sect. 5.4.9 when two messages are sent through independent transceivers.

4.1.4.4 Black channels

An interesting concept in the standard is the use of "black channels." Note that a "white channel" is a communications channel that consists entirely of (expensive) safety-grade equipment. A black channel is a communications channel that carries safety-related messages but is not itself safety-grade.[8] Its use in a safety-related communications channel is justified by adding the SCL prescribed by the standard. The SCL is present at both black channel end-points as shown in Fig. 4.5. The SCL performs safety-related transmission functions and checks on the communication to ensure that the integrity of the link meets its requirement. Having detected a problem, the SCL corrects it or, failing that, puts the system into a safe state (e.g., by tripping the reactor).

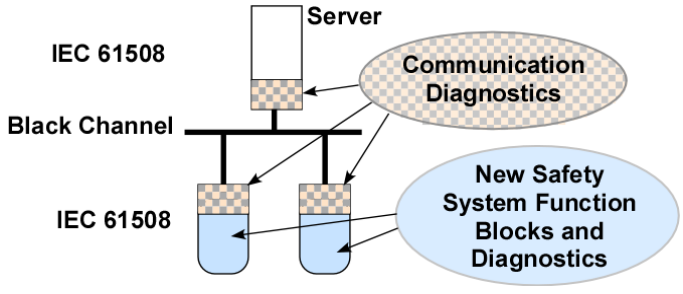

Fig. 4.5. Illustration of black channel implementation.

The need for equipment such as network repeaters, bridges, hubs, switches, and routers might motivate a black channel implementation. A possible black channel example would be shared communication of both safety- and nonsafety-related process input signals on the same media leaving reactor containment. The safety-related signals would require SCLs at both sending and receiving ends. In the event that the SCL detected a communications error, there would be an attempt to correct the error (e.g., retransmit a lost message). Should that fail, the SCL at both ends would be obliged to assume that an unsafe condition exists and perform the safety functions determined by their design. This function might be to cast a vote for an actuator movement; a simple control room display receiving process signals might indicate the communications loss on that division to the operator.

4.1.4.5 Security perspective

The standard includes the observation:

> "All systems are exposed to unauthorized access at some point of their life cycle."

In this case, unauthorized access includes non-malicious accidents such as can occur during installation, operation, maintenance, or most any other time. A safety system can be exposed to malicious attacks through data paths that breach its isolation boundary. For example, digital media from a vendor's computer that is on the Internet can carry malicious software to a plant computer used for safety system maintenance. That malicious software could then infect the safety system when connected during maintenance. This scenario becomes more likely should commercially accepted systems be used in nuclear power plants. The IEC 61784 standard, which defers to IEC 62443 on issues of security, also addresses the vulnerability of black channel implementations:

> When an application requires electronic security measures, the security shall be implemented within the black channel. The security function can be implemented either within the devices, or at external access points. Some requirements for security are detailed in IEC 62443.

Cybersecurity as it relates to communications between safety and nonsafety systems is an important issue that is beyond the scope of this report. It nevertheless must be considered in the review of communications systems. A recommendation is to launch an investigation into related current work and standards including IEC 61784-4, which has just started development.

4.2 SUMMARY OF CONSENSUS PRACTICES

The standards and guides discussed advocate design guidance that considers many reasonable influences on digital communications related to safety functions. The high reliability requirement of a nuclear safety system design leads to design attributes such as the following.

The system should be isolated and independent to the extent possible. This includes physical isolation (e.g., electrical, environmental, etc.) and functional isolation (e.g., data transfer with nonsafety systems). Interaction through isolation barriers should be one-way, from the safety system, not to the safety system. Specifically for communications, the safety function should not be impaired by communications failures.

The isolation and independence strategies are applied so that, to the extent required, each safety system is isolated and independent from (1) nonsafety systems, (2) different channels with the same safety function, (3) other layers of defense with the same safety function, and (4) other classes of safety systems.

The system should be simple so that the probability that it contains hidden flaws due to requirements or design errors is minimized. A particular concern is that common-cause failure will

disable a safety system based on multiple channels of identical equipment. Simplicity in communications is achieved through a fixed, periodic schedule for network communications (thus, avoiding network congestion). The reliability requirements will require that communications failures such as lost messages be considered. This can be done through retransmission at intervals allotted in the schedule. An even simpler strategy, useable if the network routinely transmits frequently enough, is to wait for the next transmission.

The design should be such that it can be demonstrated that the system will respond with a required safety action within the time required, despite credible failures.

The SCL is a new communications layer, added to the standard OSI layer model, which is charged with guaranteeing that all safety-related communications passed between network nodes are detected. Upon detection, the SCL's job is to remedy the errors or put the system into a safe state with the response time required. The black channel is an associated concept that allows nonsafety equipment to be part of a safety communications network, provided any errors caused by the nonsafety equipment are handled by the SCL. These concepts allow communications buses to be adapted to safety-related functions by adding an SCL to the existing product, rather than redesigning the product.

Security is typically enforced through physical access controls. For example, keyed interlocks prohibit access to a node that is operating in maintenance or set point update mode. A detailed security methods study is outside the scope of this letter report. However, it is worth noting that security for industrial instrument networks is driven by different concerns than information technology (IT) networks. For example, industrial networks need to protect the end nodes (instruments), while the IT is usually concerned with protecting the central nodes (servers) from the end nodes (personal computers). Such differences are driving the creation of a different standard.

REFERENCES

1. G. Johnson, Comparison of IEC and IEEE Standards for Computer-Based Control Systems Important to Safety, UCRL-ID-146642, Lawrence Livermore National Laboratory, 2001.
2. IEC 61500, "Nuclear Power Plants—Instrumentation and Control Systems Important to Safety—Data Communication," International Electrotechnical Commission, 2002.
3. IEC TR 61508-0, "Functional safety of electrical/electronic/programmable electronic safety-related systems—Part 0: Functional safety and IEC 61508" (working draft), International Electrotechnical Commission, Geneva, Switzerland, 2005.
4. IEC 61513, Nuclear power plants—Instrumentation and control for systems important to safety—General requirements for systems, 2001.
5. D. Fowler and P. Bennett, "IEC 61508—A Suitable Basis for the Certification of Safety-Critical Transport-Infrastructure Systems" by SAFECOMP 2000, LNCS 1943, pp. 250–263, Springer-Verlag Berlin Heidelberg 2000.
6. IEC 61784-1 Digital data communications for measurement and control—Part 1: profile sets for continuous and discrete manufacturing relative to Fieldbus use in industrial control systems, 2001.
7. IEC 61874-3 Digital data communications for measurement and control—Part 3: Profiles for functional safety communications in industrial networks, 2006.
8. EC 62280-1, "IEC 62280-1 Railway applications communication, signaling and processing systems Part 1: Safety-related communication in closed transmission systems," 1st Ed., 2002.

5. CONCLUSIONS

Of the international NPPs reviewed in this report that have implemented digital I&C technology, the use of digital communication is, in general, more pervasive than is the case for current US plants. However, those international plants that have been licensed and are currently operating do not employ digital communication to the degree being considered for some new plant designs. The evolutionary plants that are under construction internationally will provide extensive digital communication that is comparable to that provided in the new plant designs. Note that the licensing of these evolutionary plants is yet incomplete, so they represent ongoing test cases. The international licensing experience is considerable and is still evolving. Nevertheless, although some lessons can be learned from international NPPs, the international licensing experience to date, as related to digital communications, is not sufficiently conclusive to resolve the relevant open regulatory issues in the United States.

The international approach to safety classification for digital I&C systems provides for graded safety classes with increasing degrees of rigor in the design, testing, and implementation practices. Communication between systems, divisions, or modules of equivalent safety class is common. For most of the plants evaluated in this study, communication between systems of the highest safety class to systems of a lesser or nonsafety class is accomplished via isolated, buffered, one-way communication nodes. As noted in Sect. 3, Olkiluoto-3 (and the U.S. EPR) propose two-way communications between PICS and PS/SAS. Typically, communication from systems of a less stringent safety class to those of the highest safety class (i.e., RPS and ESF) is inhibited (e.g., through interlocks) unless the safety system or, more specifically, the safety division is taken out of service. The primary exception in these examples involves interface modules (e.g., priority actuation components).

The prevailing standard for the U.S. nuclear power industry on computer-based safety systems is IEEE 7-4.3.2. The standard provides guidance on maintaining independence in systems where digital communication is employed. Recognizing that its guidance on the topic can be enhanced to improve clarity and provide increased detail on specific approaches, the IEEE is considering a revision to this standard. While striving for consensus, the standards committee can benefit from broad engagement of nuclear power stakeholders, subject matter experts, and proven practices in other application domains.

Specific standards have been developed for highly reliable digital communications, architectures, and protocols. Many of these standards have arisen from the work of international committees. These standards offer high-level guidance that is generally consistent but not particularly detailed. In a few cases, a standard does provide practical recommendations for selected designs. IEC 61784-3 provides the most definitive guidance of the standards reviewed, and the nuclear power industry could benefit from considering the practices it describes. This standard was written to ensure adherence and implementation to the goals of IEC 61508.

Consensus on a single Fieldbus standard has not been achieved. The result is that the IEC 61784-3 standard contains common generic requirements and separate specific requirements for the different Fieldbus systems. Thus, the detailed guidance of IEC 61784-3 would need to be adapted for use with other communication system designs. Nevertheless, this guidance may be suitable as a basis for efficient system development and review.

The IEC 61784-3 standard adopts the SCL concept. The SCL is a communications layer, added to the standard OSI layer model, which is charged with ensuring that all safety-related communications passed between network nodes are checked and errors detected. Upon detecting an error, the SCL acts to remedy the errors or put the system into a safe state within the required response time. The black channel, endorsed by IEC 61784-3, is an associated concept that allows equipment not built to safety related standards to be part of a safety communications network, provided any errors caused by the

nonsafety equipment are handled by the SCL. This approach assigns a significant responsibility to the SCL.

The SCL introduces a divide-and-conquer strategy to the design of safety communications: it divides the safety problem into communications and non-communications issues, with the SCL specifically focused on the communications issues. Problems arising from sources other than communications performance, such as safety application logic and physical isolation, are handled elsewhere. The communications problem becomes one of determining that intact messages are arriving on schedule, correcting errors where possible, and putting the system into a safe state when communications fail. The standard addresses the first two tasks but does not provide much guidance about specific measures to accomplish the third task. If determining a safe state is nontrivial and communications errors have made the available data suspect, then the SCL may not be able to readily identify which state is safe. The definition of the SCL must address establishment of an unambiguous safe state. Determining a safe state is application dependent and is not addressed directly by the standard. The safe state must be determined by a design engineer and safety analysis of the impact of the communication failure on the state of the plant. Methods for doing this are defined in IEC 61508 or sub-tier application-specific IEC standards.

The SCL has the responsibility for isolating the safety system from the informational errors possible in the black (nonsafety) communications channel. This capability has the potential for facilitating safety communications over nonsafety communications links or enabling the shared use of a safety Fieldbus with nonsafety devices. However, this investigation did not find any examples demonstrating whether designs adhering to the IEC 61784-3 standard also can meet the high reliability (Safety Integrity Level) goals associated with nuclear safety applications.

Knowledge of the specific network architecture used in safety-to-safety and nonsafety-to-safety communication, including abstraction layers and interconnectivity (topology of source and receivers), enables identification of potential communication errors and vulnerabilities. Methods of error mitigation and means of limiting error propagation to the safety function depend on understanding those anticipated errors and the expected types of safety messages. Industrial knowledge and experience exists for an extensive range of communication error types and fault handling approaches. Whether and how well error and failure types are addressed should be considered in the evaluation of nuclear safety system designs. Some topologies require more design and implementation effort to be suitable for safety systems. Network bus topologies can provide appropriate determinism and reliability although the review of safety characteristics of such systems is more complex.

A structured approach for evaluation of safety-to-safety and nonsafety-to-safety communications systems has emerged from this study and can be summarized as follows. From Sect. 2, two general failure categories can be considered: (1) information and (2) communication. Information failure encompasses any situation in which a message or data to a safety system appears valid but is wrong (e.g., incorrect, misguided). A communication failure refers to the loss of messages or data as a result of transmission. As shown in Fig. 5.1, these failure categories can lead to two outcomes:
(1) interruption of safety function execution (i.e., code execution stops or is impeded) or (2) incorrect performance of the safety function (i.e., incorrect decision). These conditions result from executional and/or functional dependence of the safety division on networked information from external sources and are not consistent with the independence design criterion. A communication buffer between the bus or network and safety function processor should be implemented to ensure that normal execution is not impeded by attention to external communication duties. Incorrect data from other safety or nonsafety systems should not lead to an incorrect safety decision. Where external communication is necessary, functional dependence can be minimized if the implementation can accommodate erroneous, corrupted, or unanticipated information. Independence can be promoted by controlling the pass-through of information based on strict message formalism and validity checks.

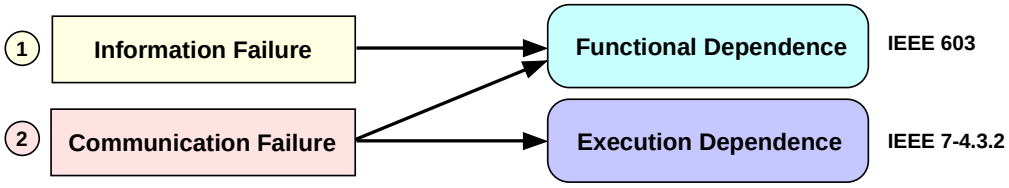

Fig. 5.1. Simple evaluation approach for safety systems communications.

Appendixes

Appendix A.
OSI SEVEN-LAYER MODEL

Communications layer	Description
Application *Layer 7*	This layer supports application and end-user processes. Communication partners are identified, quality of service is identified, user authentication and privacy are considered, and any constraints on data syntax are identified. Everything at this layer is application-specific.
Presentation *Layer 6*	This layer provides independence from differences in data representation (e.g., encryption) by translating from application to network format and vice versa. The presentation layer works to transform data into the form that the application layer can accept. This layer formats and encrypts data to be sent across a network, providing freedom from compatibility problems. It is sometimes called the *syntax layer*.
Session *Layer 5*	This layer establishes, manages, and terminates connections between applications. The session layer sets up, coordinates, and terminates conversations, exchanges, and dialogues between the applications at each end. It deals with session and connection coordination.
Transport *Layer 4*	This layer provides transparent transfer of data between end systems, or hosts, and is responsible for end-to-end error recovery and flow control. It ensures complete data transfer.
Network *Layer 3*	This layer provides switching and routing technologies, creating logical paths, known as virtual circuits, for transmitting data from node to node. Routing and forwarding are functions of this layer, as well as addressing, internetworking, error handling, congestion control, and packet sequencing.
Data Link *Layer 2*	At this layer, data packets are encoded and decoded into bits. It furnishes transmission protocol knowledge and management and handles errors in the physical layer, flow control, and frame synchronization. The data link layer is divided into two sublayers: the Media Access Control (MAC) layer and the Logical Link Control (LLC) layer. The MAC sublayer controls how a computer on the network gains access to the data and permission to transmit it. The LLC layer controls frame synchronization, flow control, and error checking.
Physical Interface *Layer 1*	This layer conveys the bit stream—electrical impulse, light, or radio signal—through the network at the electrical and mechanical level. It provides the hardware means of sending and receiving data on a carrier, including defining cables, cards, and physical aspects. Fast Ethernet, RS232, and ATM are protocols with physical layer components.

Appendix B.
COMMUNICATION-RELEVANT EXCERPTS FROM TITLE 10 CFR PART 50, APPENDIX A

Pursuant to the provisions of §50.34, an application for a construction permit must include the principal design criteria for a proposed facility. The principal design criteria establish the necessary design, fabrication, construction, testing, and performance requirements for structures, systems, and components important to safety; that is, structures, systems, and components that provide reasonable assurance that the facility can be operated without undue risk to the health and safety of the public.

These General Design Criteria establish minimum requirements for the principal design criteria for water-cooled nuclear power plants similar in design and location to plants for which construction permits have been issued by the Commission. The General Design Criteria are also considered to be generally applicable to other types of nuclear power units and are intended to provide guidance in establishing the principal design criteria for such other units.

The following General Design Criteria are relevant to communications between safety divisions and between safety and nonsafety systems.*

Criterion 20. Protection System Functions

The protection system shall be designed (1) to initiate automatically the operation of appropriate systems, including the reactivity control systems, to assure that specified acceptable fuel design limits are not exceeded as a result of anticipated operational occurrences and (2) to sense accident conditions and to initiate the operation of systems and components important to safety.

Criterion 21. Protection System Reliability and Testability

The protection system shall be designed for high functional reliability and in-service testability commensurate with the safety functions to be performed. Redundancy and independence designed into the protection system shall be sufficient to assure that (1) no single failure results in loss of the protection function and (2) removal from service of any component or channel does not result in loss of the required redundancy unless the acceptable reliability of operation of the protection system can be otherwise demonstrated. The protection system shall be designed to permit periodic testing of its functioning when the reactor is in operation, including a capability to test channels independently to determine failures and losses of redundancy that may have occurred.

Criterion 22. Protection System Independence

The protection system shall be designed to assure that the effects of natural phenomena and of normal operating, maintenance, testing, and postulated accident conditions on redundant channels do not result in loss of the protection function, or shall be demonstrated to be acceptable on some other defined basis. Design techniques, such as functional diversity or diversity in component design and principles of operation, shall be used to the extent practical to prevent loss of the protection function.

Criterion 23. Protection System Failure Modes

The protection system shall be designed to fail into a safe state or into a state demonstrated to be acceptable on some other defined basis if conditions such as disconnection of the system, loss of energy (e.g., electric power and instrument air), or postulated adverse environments (e.g., extreme heat or cold, fire, pressure, steam, water, and radiation) are experienced.

---

*Other General Design Criteria are important for safety systems as well including 10, 13, 15, 16, 19, 27, 28, 34, 35, 37, 38, 40, 41, 43, 56, and 57.

Criterion 24. Separation of Protection and Control Systems

The protection system shall be separated from control systems to the extent that failure of any single control system component or channel, or failure or removal from service of any single protection system component or channel, which is common to the control and protection systems, leaves intact a system satisfying all reliability, redundancy, and independence requirements of the protection system. Interconnection of the protection and control systems shall be limited so as to assure that safety is not significantly impaired.

Criterion 25. Protection System Requirements for Reactivity Control Malfunctions

The protection system shall be designed to assure that specified acceptable fuel design limits are not exceeded for any single malfunction of the reactivity control system, such as accidental withdrawal (not ejection or dropout) of control rods.

Criterion 29. Protection Against Anticipated Operational Occurrences

The protection and reactivity control systems shall be designed to assure an extremely high probability of accomplishing their safety function in the event of anticipated operational occurrences.

Appendix C.
TRIGGERS FOR COMMUNICATIONS ERRORS

The following are considered root causes for communication errors and poor network performance based on common industrial experience. Consideration of error types and faults are useful during design evaluation to look for potential failure mechanisms arising from architecture, protocols, or design-specific details.

1. EXCESSIVE COLLISIONS—Excessive bandwidth utilization and message collisions. This is a design-related issue. During a plant event or due to some other change, the network becomes congested because the design architecture and implementation did not consider it.
2. BAD CABLING—Intermittent or faulty cabling, connectors, and switches. Random failure or environmental effects due to physical interface. Incorrectly made physical connections are also a possibility.
3. FAULTY NETWORK CARDS—Faulty network interface cards (NICs), which are at the physical interface. Random failure or environmental effect. Could be more complicated failure mode than item 2 above—bad node address could be generated and/or used.
4. PROTOCOL INCOMPATIBILITIES—Incomplete testing of new products (or product revisions) to match standard protocols (i.e., *bugs*). Incompatibility; design/implementation signal timing issues.
5. TIMING VARIABILITY—Poor deterministic performance from variable cycle timing. This design timing issue can be avoided according to IEC 61500. However, some timing variations are permissible, such as sequence of event logging functions handling a burst of plant alarms.
6. PACKET CORRUPTION—Environmental noise (e.g., EMI) that corrupts data and introduces errors. This is a physical layer and handshaking issue.
7. FAULTY GATEWAY—Incomplete or faulty network gateway. This would be a gateway between the safety and nonsafety networks. A gateway in the sense of a translator between networks operating under different protocols, or in the sense of a bridge between different physical media in the same logical network. This could be a nonsafety-grade performance monitoring and logging system attached to the safety-grade nodes (e.g., TELEPERM™ service unit computer[*]).
8. DUPLICATE ADDRESSES—Duplicate network addresses. This problem can arise from installation or maintenance actions or because of run-time errors that change a node's address. It is generally handled by installation/maintenance procedures, or by robust run-time handshaking/routing.
9. EXCESSIVE LOADING—Excessive loading of a network due to node access from external sources (e.g., from human interface device such as control room console). With arbitrary access can come excess network loading. Other factors include a malfunction at the workstation console (e.g., nonsafety grade) that errantly accesses the network frequently. During a plant event, many data requests are expected that would load the network. Examples include high-speed variable tracking and multiple operators.
10. EXCESSIVE BROADCASTING—Excessive loading of a network due to broadcast messaging. This issue must be addressed during design. Simplex broadcasting avoids tie ups from handshaking but still loads the network.
11. UNAUTHORIZED ACCESS—Unauthorized access of digital controllers (e.g., PLCs). The presumption is that unauthorized access leads to configuration or parameter changes so that its operation is affected. This issue relates to physical lockouts (i.e., locks and keys) or software

[*]For TXS (used for Olkiluoto-3 and the US EPR), the MSI is safety related, and the service unit is nonsafety related.

lockouts (i.e., operating system prevents configuration change messages unless the node is in configuration mode).

12. INCORRECT DEVICE—Installation of the wrong product or wrong protocol version of the product. This is an installation and maintenance issue.