U.S.NRC

United States Nuclear Regulatory Commission

Protecting People and the Environment

NUREG/CR-6991
ONRL/TM-2007/184

Design Practices for Communications and Workstations in Highly Integrated Control Rooms

Office of Nuclear Regulatory Research

AVAILABILITY OF REFERENCE MATERIALS IN NRC PUBLICATIONS

NRC Reference Material

As of November 1999, you may electronically access NUREG-series publications and other NRC records at NRC's Public Electronic Reading Room at http://www.nrc.gov/reading-rm.html. Publicly released records include, to name a few, NUREG-series publications; *Federal Register* notices; applicant, licensee, and vendor documents and correspondence; NRC correspondence and internal memoranda; bulletins and information notices; inspection and investigative reports; licensee event reports; and Commission papers and their attachments.

NRC publications in the NUREG series, NRC regulations, and *Title 10, Energy*, in the Code of *Federal Regulations* may also be purchased from one of these two sources.

1. The Superintendent of Documents
   U.S. Government Printing Office
   Mail Stop SSOP
   Washington, DC 20402–0001
   Internet: bookstore.gpo.gov
   Telephone: 202-512-1800
   Fax: 202-512-2250
2. The National Technical Information Service
   Springfield, VA 22161–0002
   www.ntis.gov
   1–800–553–6847 or, locally, 703–605–6000

A single copy of each NRC draft report for comment is available free, to the extent of supply, upon written request as follows:

Address: Office of Administration
Reproduction and Mail Services Branch
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001
E-mail: DISTRIBUTION@nrc.gov
Facsimile: 301–415–2289

Some publications in the NUREG series that are posted at NRC's Web site address http://www.nrc.gov/reading-rm/doc-collections/nuregs are updated periodically and may differ from the last printed version. Although references to material found on a Web site bear the date the material was accessed, the material available on the date cited may subsequently be removed from the site.

Non-NRC Reference Material

Documents available from public and special technical libraries include all open literature items, such as books, journal articles, and transactions, *Federal Register* notices, Federal and State legislation, and congressional reports. Such documents as theses, dissertations, foreign reports and translations, and non-NRC conference proceedings may be purchased from their sponsoring organization.

Copies of industry codes and standards used in a substantive manner in the NRC regulatory process are maintained at—

The NRC Technical Library
Two White Flint North
11545 Rockville Pike
Rockville, MD 20852–2738

These standards are available in the library for reference use by the public. Codes and standards are usually copyrighted and may be purchased from the originating organization or, if they are American National Standards, from—

American National Standards Institute
11 West 42nd Street
New York, NY 10036–8002
www.ansi.org
212–642–4900

Legally binding regulatory requirements are stated only in laws; NRC regulations; licenses, including technical specifications; or orders, not in NUREG-series publications. The views expressed in contractor-prepared publications in this series are not necessarily those of the NRC.

The NUREG series comprises (1) technical and administrative reports and books prepared by the staff (NUREG–XXXX) or agency contractors (NUREG/CR–XXXX), (2) proceedings of conferences (NUREG/CP–XXXX), (3) reports resulting from international agreements (NUREG/IA–XXXX), (4) brochures (NUREG/BR–XXXX), and (5) compilations of legal decisions and orders of the Commission and Atomic and Safety Licensing Boards and of Directors' decisions under Section 2.206 of NRC's regulations (NUREG–0750).

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

NUREG/CR-6991
ORNL/TM-2007/184

Design Practices for Communications and Workstations in Highly Integrated Control Rooms

Manuscript Completed: February 2009
Date Published: September 2009

Prepared by
R. Kisner, D. Holcomb, J. Mullens, T. Wilson,
R. Wood, K. Korsah, M. Muhlheim, A. Qualls,
M. Howlader, G. Wetherington, Jr.,
P. Chiaro, Jr., and A. Loebl

Oak Ridge National Laboratory
P.O. Box 2008
Oak Ridge, TN 37831-6075

P.J. Rebstock, NRC Project Manager

NRC Job Code N6350

Office of Nuclear Regulatory Research

ABSTRACT

This report presents the findings and observations obtained in the course of the associated research and does not indicate NRC endorsement of the designs and methods reported. The Foreword to this report provides additional information concerning this subject.

This report presents the results of research used in the development of review guidance and associated acceptance criteria for use by regulatory staff in confirming that highly integrated control room (HICR) designs are in conformance with Nuclear Regulatory Commission (NRC) requirements. The principal features of the HICR are extensive use of digital network communications and digital operator workstations. The purpose of this report is to document technical considerations that support the development of guidance that specifically addresses issues related to communication among safety divisions and between safety-related equipment and equipment that is not safety related. This information is intended to provide clarification in recognition of the possible variations in digital-communication-based systems.

Documents such as IEEE 7-4.3.2, Regulatory Guide 1.152, and IEEE 603 (considered current industry and NRC guidance) are not sufficiently detailed for evaluating interdivisional communications independence. Thus, the NRC seeks to establish evaluation criteria for safety systems communications that can be uniformly applied in a variety of safety system designs.

The report examines (1) operating experience and lessons learned, (2) accepted consensus practices, and (3) analysis of credible failure mechanisms arising from several possible network architectures and message types. A structured approach for evaluation of safety-to-safety and nonsafety-to-safety communications systems has emerged from this study. 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 because of transmission.

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

FOREWORD

The highly integrated control rooms proposed for new reactors will be very different from control rooms in existing domestic nuclear power plants (NPP). The large benchboards and consoles housing hardwired controls and indicators in the existing NPP will be replaced in new reactors by computer-operated displays and soft controls implemented by touch-screen or other technologies. This follows a trend already established and well under way in other industries involving complex and safety-critical processes.

The objective of the research project presented in this report was to explore the approach to safety-significant digital systems used in other industries and in other countries, and to examine whether and how nonsafety equipment and equipment in different safety divisions may be connected together and permitted to communicate.

In addition to the research project described herein, NRC initiated an internal Digital I&C Project to address various specific aspects of the implementation and licensing of digital systems used in safety-related applications in domestic NPP and related facilities. Part of that project, designated "Task Working Group 4" (TWG4), addressed the subject of digital communications among redundant safety divisions and between safety and nonsafety divisions. TWG4 addressed licensing-related design considerations involving communications among safety-related divisions and between safety and nonsafety divisions. The findings of TWG4 were incorporated into a guidance document intended for use by both applicants and NRC reviewers. This document established the NRC staff position on these subjects and will be used as guidance in the review and licensing of safety-related digital systems. The guidance document is Interim Staff Guidance DI&C-ISG-04 (ISG4), *Interim Staff Guidance on Highly-Integrated Control Rooms—Communications Issues (HICRc)*, issued September 28, 2007.

This NUREG/CR presents Oak Ridge National Laboratory's findings from research performed on behalf of the NRC. The information gathered was used in the development of ISG4, although publication of ISG4 preceded publication of this report. It should be noted that this report presents information concerning some practices and design features that are not consistent with the guidance presented in ISG4: that information is included here in the interest of complete reporting of the contractor's findings, and it does not supersede the positions expressed in ISG4. ISG4 presents the NRC's position on matters concerning digital communications involving safety related functions, and in the event of apparent conflict between ISG4 and any aspect of this report, ISG4 shall prevail.

CONTENTS

APPENDICES

LIST OF FIGURES

LIST OF TABLES

EXECUTIVE SUMMARY*

Purpose

Oak Ridge National Laboratory (ORNL) has been engaged by the U.S. Nuclear Regulatory Commission (NRC) Office of Nuclear Regulatory Research (RES) to perform research to be used in the development of review guidance and associated acceptance criteria for use by regulatory staff in confirming that highly integrated control room (HICR) designs are in conformance with NRC requirements. Distinctive HICR features are extensive use of digital network communications and digital operator workstations. These features provide operations flexibility and potentially increase operations and maintenance efficiency. However, depending on design methodology and implementation, new failure modes are possible. The preference of both NRC and industry is that guidance be provided that would minimize detailed open-ended, case-by-case reviews of every plant system. This report documents technical information used in the development of guidance that specifically addresses issues related to communication among safety divisions and between safety-related equipment and equipment that is not safety related. This report is intended to provide clarification in recognition of the variety of communication configurations and topologies possible between digital-communication-based systems.

Current industry and NRC guidance documents such as 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. Note that this report does not provide design guidance, nor does it present detailed failure modes and effects analysis (FMEA) results for existing designs.

This report presents the findings and observations obtained in the course of the associated research and does not indicate NRC endorsement of the designs and methods reported or recommended. The Foreword to this report provides additional information concerning this subject.

Methods

Three elements are considered necessary to establish a detailed technical basis for regulatory guidance: (1) operating experience and lessons learned, (2) accepted consensus practices, and (3) analysis of credible failure mechanisms. Operating experience relative to digital workstations and network communications has been drawn principally from international power reactors because of limited digital communication implementation in U.S. nuclear power plant (NPP) safety systems. Industry standards such as Institute of Electronic and Electrical Engineers (IEEE) and International Electrotechnical Commission (IEC) have been reviewed as a part of determining accepted consensus practices. To analyze potential failure mechanisms, digital network communication failures were studied, especially examining architectures that might be considered in nuclear safety systems. A taxonomy of error types, message types, and failure mechanisms was developed.

Results

The following sections of this Executive summary address recommendations that are presented in the main body of this document. Those recommendations were taken into consideration in the

*Publications that are referred to in this Executive Summary also appear in the main body of this report and are cited as references.

development of NRC guidance on these matters. Some recommendations may not have been incorporated into the guidance, and some may have been incorporated in an altered form. The NRC guidance may also include provisions not addressed here. These results do not themselves constitute NRC guidance on these matters.

Communication Vulnerabilities

The communications vulnerabilities section describes key configuration and performance aspects of digital communication systems. A generic safety-systems configuration model is described including bus, serial, and network communications within the system. Division-to-division, safety-to-safety, and nonsafety-to-safety communications are discussed relative to the generic model. Background information on the fundamentals of communications and communication vulnerabilities as they relate to nuclear safety applications is examined in some detail. The issue of digital data communication between safety systems can be summarized by two failure conditions: (1) loss of communication—a failure to communicate any necessary data when it is needed and (2) creation of erroneous information that has the potential to be received and to subsequently elicit incorrect actions. Data (or the lack thereof) from any source should not inhibit a safety system from performing its designated function.

Communications networks that connect safety-grade systems to other safety-grade systems will be themselves considered safety grade and with the associated isolator should be designed to safety criteria. Nonsafety portions of a communication network do not have to be designed to safety criteria. 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). Properly isolated 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.

Communication network architectures are examined from several perspectives. The Open Systems Interconnection (OSI) seven-layer model for network communications is used as a paradigm for the transmission of messages between network nodes. The seven-layer model is condensed to three layers, which is more representative of digital communications between instrumentation and control systems in nuclear power and other industrial applications. Several network topologies are described and discussed including the simple but prevalent point-to-point as well as network buses and segmented networks. A brief overview of signal multiplexing and network synchronization is provided.

Communication, both human and electronic, is fundamentally about sending and receiving information and for the intent of this topical report, it is about the delivery of information from a source to one or more receivers. In a world without bandwidth limits, noise, transients, component faults, and errors, information would be correctly assembled and coded at the source then transmitted to the receiver; at the receiver, that information would be decoded and used correctly. Unfortunately, failures and errors can and do appear in numerous places along the path from source to receiver. Possible sources from which errors may be introduced into the system include (1) signal source-generated errors, (2) communication/transmission-channel-generated errors (including interposed bridges and routers), (3) signal receiver–generated errors, and (4) system-wide, component-interaction-generated errors. A taxonomy of network error types has been extracted from numerous sources. By combining signal source and receiver in one category, three general categories of error types have been identified: communications, sender/receiver, and segmented network. The error types are shown in the table below. The report describes each in detail with examples. The interaction of these errors with each of the three communication layers is described. Defensive measures, which are drawn from international standards, are matched with the error types. The defensive measures are then described.

Six categories of message data are described that cover the bulk of safety-to-safety and nonsafety-to-safety communications. These categories are described with examples. The potential effect of errors in the message types and possible methods to mitigate those effects are described as well.

The method of handling error and failure types should be considered in the evaluation of nuclear-safety-system designs. Error mitigation methods and means to limit error propagation to the safety function depend on understanding the anticipated errors and the expected types of safety messages. Some communication networking topologies require more design and implementation effort to be suitable for safety systems. Knowledge of the specific network architecture enables identification of potential communication vulnerabilities. Industrial knowledge and experience exist for an extensive range of communication error types and fault-handling approaches.

Communications-related errors
Corruption
Unintended Repetition
Incorrect Sequence
Loss
Unacceptable Delay
Insertion
Masquerade
Addressing
Broadcast Storm
Babbling Idiot (Commission Fault)
Inconsistency (Byzantine Generals' Problem)
Excessive Jitter
Collision
Sender/receiver-related errors
Buffer Overflow
Data Out of Range
Incorrect Ordering
Message Too Early
Encoding/Decoding
Segmented-network-related errors
Very Long Delays in Bridges and Routers
Very Long Times to Initiate Communications
Complete Blockage

The network error and defensive measure strategies support the review process by enabling identification, screening, and assessment of capabilities, characteristics, and strategies to ensure high-integrity, dependable communication for safety-relevant applications. Three steps are associated with this review process: (1) identify architecture and topologies used and note their key characteristics, (2) screen known vulnerabilities to define a credible set applicable to the architecture, and (3) assess the application of defensive solutions and their strategies to mitigate the vulnerabilities.

International Power Reactor Experience

The use of digital communication is, in general, more pervasive in the international NPPs reviewed in this report than is the case for current U.S. plants. However, those international plants do

not employ digital communication on the scale being considered for some new U.S. plant designs. The evolutionary plants that are under construction internationally will provide extensive digital communication comparable to the new U.S. plant designs. However, the licensing of these evolutionary plants is incomplete and evolving. 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, although some lessons can be learned from international NPPs.

A brief description is given in the report of the graded safety-system classification schemes supported by different international nuclear power regulatory bodies. 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. All other nuclear safety bodies employ a more finely divided safety classification system. Communication between systems of equivalent safety classes is generally allowed. 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 buffered, one-way communication nodes. As noted in Sect. 3, Olkiluoto-3 (and the U.S. EPR) propose two-way communications between the Process Information and Control System (PICS) and the Protection System/Safety Automation System (PS/SAS). Typically, communication from systems of a less stringent safety class to those of the highest safety class [i.e., reactor protection system (RPS) and engineered safety feature (ESF)] is inhibited (e.g., through interlocks) unless the safety system or, more specifically, the safety division is taken out of service. The sole exception in these examples involves interface modules (e.g., priority actuation components).

Seven international power reactors are examined: Chooz B (France), Sizewell B (United Kingdom), Darlington (Canada), Lungmen (Taiwan), Temelin (Czech Republic), Dukovany (Czech Republic), and Olkiluoto-3 (Finland). The goal of the investigation was to identify (a) the logical communication structures, (b) the technology involved, (c) the communication segregation strategy for functional diversity, (d) the redundant communication links to reduce 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 review addresses the strategies of different vendors to ensure overall reliability of the communications system. These include techniques to ensure that failure rates of individual links are very low and that there is no common cause failure in the communications systems that compromises the function of the safety system. No proprietary data are disclosed in the report.

Both U.S. and international nuclear power regulatory bodies make available their regulatory principles for digital communication architectures. Acceptance criteria for digital communication topologies, however, provide little guidance as to whether any particular implementation methodology offers reasonable assurance for achieving them. The international consensus standard on NPPs—*Instrumentation and control for systems important to safety—General requirements for systems* (IEC 61513)—specifically limits its scope to not include additional national regulations. Further, while probabilistic analysis as a means for achieving reasonable assurance is becoming more common in design and analysis tools, probabilistic digital system analysis has not been fully embraced by any nuclear power regulatory authority.

A few consensus regulatory practices have emerged from investigating experiences with international digital I&C systems. Communications with the highest grade of safety system are always from a high-quality, regulated system but not necessarily from the highest class of safety system. The highest class safety system must be in bypass to accept communication access for all but the simplest communications (e.g., protocol handshaking). Both logical and physical access controls are universally employed for implementing changes to safety system performance. In some cases, software updates can be performed following a physical enable with the hardware installed and bypassed. In others, physical hardware replacement is required to perform software upgrades.

The U.S. regulatory process is presented with advanced digital system architectures with only a limited version of the two to three decades of gradual adoption of digital I&C performed in other nuclear power nations. To some extent, this situation in the United States has come about because of its period of dormancy in NPP construction (and to a large extent even upgrades). As a counter example, Japanese and French NPPs have adopted digital technology into safety applications as part of a gradual progression from application in subsidiary, nonsafety systems, to control systems, to lower class safety systems, to top-tier safety systems. With two safety categories (safety and nonsafety), gradual progression of digital topologies into U.S. NPP safety systems has been limited.

Consensus Practices from Nuclear and Non-Nuclear Applications

The report section dealing with consensus practices examines a selected set of standards concerning a variety of aspects of digital communications for instrumentation and control. The purpose of this section is to collect accepted practices from them. Documents reviewed include IEEE 603-1998, IEEE 7-4.3.2-2003, IEC 61500, IEC 61508, IEC 61511, IEC 61513, IEC 61784-3, VTT Research Notes 2265, and the European Workshop on Industrial Computer Systems (EWICS) TC7. Other useful documents include IEC 60880-2006 and IEC 61226-2005.

For the U.S. nuclear power industry, the prevailing standard on computer-based safety systems is IEEE 7-4.3.2, which provides guidance on maintaining independence in systems where digital communication is employed. The IEEE is considering a revision to this standard to enhance guidance on the topic and to improve clarity and provide increased detail on specific technical approaches,. As the standards committee progresses toward an improved standard, it can benefit from engagement of nuclear power stakeholders, subject matter experts, and proven practices in other application domains.

Specific standards, which have been developed for highly reliable digital communications, architectures, and protocols, have followed from the work of international committees. These standards offer high-level guidance that is generally consistent but not particularly detailed. IEC 61784-3, which provides the most definitive communications guidance of the standards reviewed, is examined in some detail with respect to hard real-time responses, the safety-related communication layer, safety measures, data integrity calculations, and black channels. This standard was written to ensure adherence and implementation to the goals of IEC 61508. The IEC 61784-3 standard introduces the Safety Communication Layer (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. The SCL, which is described in more detail in the report, does not appear to be appropriate for the highest safety class.

The collection of standards reviewed provide design guidance that considers many influences on digital communications related to safety functions. The high reliability requirement of a nuclear safety system design leads to particular design attributes such as the following:

- A safety system should be isolated and independent to the maximum extent possible using physical isolation (e.g., electrical, environmental, etc.) and functional isolation (e.g., data transfer with nonsafety systems). Interaction between safety and nonsafety systems through isolation barriers should be one way, from (not to) the safety system. Most importantly, the safety function should not be impaired by communications failures. Isolation and independence strategies are applied so that each safety system is isolated and independent from (1) nonsafety systems, (2) different divisions 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 to minimize the probability that it contains hidden flaws attributable to requirements or design errors. A top-level concern is that common-cause failure will disable a safety system that has been constructed using 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 require that communications failures such as lost messages be considered.

- 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.

Cybersecurity

Early NPP safety system designs that used analog voltages and currents to communicate trip status were more secure than modern digital networks because each circuit only connected two systems, was electrically isolated, and conveyed only a low-information-content, representative signal. The nuclear power industry, however, is being driven by technology progression to the replacement of obsolete point-to-point analog communication topologies with more capable digital networks. Although digital communication benefits are great, the network can potentially become a high-speed conduit of computer security threats including viruses, malware, and unauthorized user access. Because of this potential, a safety system that utilizes networking technology for interdivisional communications should address cybersecurity issues to the same level as any other network components of the safety system. Both external and insider attacks should be considered.

The best approach to protect systems that perform safety functions from cyberattacks is to isolate them. The design and implementation should avoid any kind of remote configuration. Encryption technologies should be used to secure information transfer originating external to the safety system. If communication is required to external systems, especially nonsafety-related systems, communication implementation from within the safety system should be done such that the communication is under safety system control. Ideally, the safety system should use unidirectional communication only (e.g., information dissemination instead of information being gathered from nonsafety systems). Recommendations for specific guidance are provided related to interdivisional network communications and external (nonsafety) network communications.

Equipment Qualification

Recommended equipment qualification review guidance and recommended acceptance criteria for communication reliability for workstations (e.g., visual displays and controls) is described in Sect. 5 as derived from Regulatory Guide 1.152, Regulatory Guide 1.209, Regulatory Guide 1.180, IEEE Standard 603, IEEE Standard 7-4.3.2, Military Standard MIL-STD-461E, and IEC 61000 series of EMI/RFI test methods. An attempt has been made to ensure that the recommendations provided in this section do not contradict existing regulatory guidance or requirements.

Specific guidance is proposed for communication architectures and operator interfaces:

- interdivisional communications,
- multidivisional control and display stations,
- safety-related stations that receive information from other divisions that are either safety or nonsafety related,
- safety-related stations controlling or monitoring the operation of equipment in safety-related divisions,
- nonsafety stations controlling or monitoring the operation of equipment in safety-related equipment, and
- nonsafety stations receiving information from safety division(s).

A Structured Methodology for Evaluation of Communications

A structured approach for describing the vulnerabilities of safety-to-safety and nonsafety-to-safety communications systems has emerged from this study. As previously discussed, the issue of digital data communication to a safety system is characterized by two failure scenarios: (1) creation of erroneous information and (2) loss of 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. 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). A remedy is to employ a communication buffer between the bus or network and safety function processor to ensure that normal execution is not delayed or impeded by attention to external communication duties; that is, incorrect data from a single other safety system or any number of nonsafety systems should not result in an incorrect safety decision. A safety function's dependence on communication correctness can be minimized by designing the receiving system to accommodate erroneous, corrupted, or unanticipated information. Communication independence can be promoted by controlling the pass-through of information.

A framework to facilitate the necessary safety review of digital communication systems for highly integrated control rooms is provided by this document and can be coupled with technical understanding of communication architectures and credible failure types. For interdivisional and nonsafety-to-safety digital communication systems, an acceptable systematic review process should address the issues posed by introducing interconnections among previously isolated systems, redundancies, and components. Certainly the communication should satisfy the essential independence criteria. Dependence on correctness of information can result in interference with the performance of a safety function; dependence on communication performance can result in preventing the fulfillment of a safety function. Recommended guidance regarding characteristics of digital communication systems that are necessary to support interdivisional and nonsafety-to-safety communication is also described in the report.

Other Supportive Information

This report contains nine appendixes describing further details of topics introduced in the report body. The appendixes cover the following subjects: (a) excerpts from 10 CFR Part 50 (Appendix A) as related to safety system network communications, (b) the Open System Interconnection (OSI) seven-layer model, (c) network multiplexing schemes, (d) triggers for communication errors, (e) relevant documents endorsed by NRC, (f) network communication timing, (g) additional review information from VTT 2265, (h) additional review guidance from the European Workshop on Industrial Computer Systems (EWICS) Guideline on Achieving Safety in Distributed Systems, and (i) elaboration on the Byzantine Generals' Logic Problem.

Conclusions

The report examines (1) accepted networking consensus practices adopted by various standards organizations in the United States and internationally, (2) operating experience of international power reactors utilizing digital network communications in safety systems, and (3) failure mechanisms associated with several possible network architectures and message types. From these information sources, recommended review guidance has been developed that pertains to interdivisional communications and nonsafety-to-safety communications. An evaluation methodology has been proposed that applies the report's findings to the regulatory review process.

ACRONYMS

ABWR	advanced boiling water reactor
ADC	analog-to-digital converter
AEPR	alarm and event processing routine
ALARA	as low as reasonably achievable
ARQ	automatic repeat request
ASIC	application-specific integrated circuit
ASM	application-specific module
AWGN	additive white Gaussian noise
BF	Browns Ferry
BPSK	binary phase shift keying
BWR	boiling water reactor
CANDU	Canadian deuterium-uranium
CASE	computer-aided software engineering
CCR	common computing resource
CCS	common core system
CCWS	component cooling water system
CDN	common data network
CDR	common computing resource
CDROM	compact disk—read-only memory
CEGB	Central Electricity Generating Board
CMOS	complementary metal oxide semiconductor
COTS	commercial off-the-shelf
CRC	cyclic redundancy check
CRT	cathode ray tube
CSMA/CD	carrier sense multiple access/collision detect
DC	data concentrator
DOE	Department of Energy
DRS	Data and Research Services
DS&S	Data Systems and Solutions
DTM	digital trip module
DVDROM	digital versatile disk—read only memory
EDT	Eastern Daylight Time
EMI	electromagnetic interference
EMS	Energy Management System
EMS	essential multiplexing system
EPR	European Pressurized Reactor
ESF	engineered safety feature
ESFAC	engineered safety feature actuation cabinet
ESL	emergency level service
EUR	European utility requirements
EWICS	European Workshop on Industrial Computer Systems
FAA	Federal Aviation Administration
FCR	fault-containment regions
FDDI	fiber distributed data interface
FDM	frequency division multiplexing
FIPS	Federal Information Processing Standards
FL	Flamanville
FM	frequency modulation

FMEA	failure modes and effects analysis
FPGA	field programmable gate array
FSK	frequency shift keying
FSL	full service level
GE	General Electric Corporation
HBS	hardwired backup system
HICR	highly integrated control room
HMI	human-machine interface
IAEA	International Atomic Energy Agency
I&C	instrumentation and control
ICS	integrated computer system
IDP	integrated display processor
IEC	International Electrotechnical Commission
IEEE	Institute of Electronic and Electrical Engineers
I/O	Input-output
IPC	Integrated Protection Cabinet
IPS	Integrated Protection System
ISS	International Space Station
IT	information technology
ITC	International Transmission Company
LAN	local area network
LCD	liquid crystal display
LLC	Logical Link Control
mA	milliamperes
MAC	Media Access Control
MDU	multifunction display unit
MEDS	multifunction electronic display system
M^2FCS	Multi-Microprocessor Flight Control System
MFD	multifunction display
MIMO	multiple-input multiple-output
MSI	Monitoring and Service Interface
MTTF	mean time to failure
mV	millivolts
NEI	Nuclear Energy Institute
NICs	network interface cards
NMR	N-modular redundant
NPP	nuclear power plant
NRC	Nuclear Regulatory Commission
NSR	nonsafety relevant
OL-3	Unit 3 of the Olkiluoto plant
OLUs	output logic units
ORNL	Oak Ridge National Laboratory
OSI	Open Systems Interconnection
PAC	Priority Actuation and Control
PAS	Process Automation System
PERFORM	performance-enhanced redundant fiber-optic replicated memory network
PICS	Process Information and Control System
PLC	programmable logic controller
PLD	programmable logic device
PS	Protection System
PSTN	public switched telephone network

PWR	pressurized-water reactor
QDS	qualified displays
RAM	random access memory
RCSL	Reactor Control, Surveillance, and Limitation
RDC	remote data concentrator
RES	Office of Nuclear Regulatory Research
RFI	radio-frequency interference
RG	Regulatory Guide
RMU	remote multiplexing units
RPS	reactor protection system
RTIF	reactor trip and isolation function
RTOS	real-time operating system
SAAS	Severe Accidents Automation System
SAS	Safety Automation System
SCL	Safety Communication Layer
SDS1 and SDS2	Shut Down System One and Two
SE	state estimator
SI	International System of Units
SICS	Safety Information and Control System
SIL	Safety Integrity Level
SNR	signal-to-noise ratio
SR	safety relevant
SRP	Standard Review Plan
STARS	Standard Terminal Automation Replacement System
TCP/IP	Transmission Control Protocol/Internet Protocol
TDM	time division multiplexing
TDMA	time-division multiple access
TLUs	trip logic units
TRIGA	Training Research and Isotope production—General Atomics
TTA	time-triggered architecture
TWG-HICRc	NRC Task Working Group on Highly Integrated Control Rooms—Communications
TXP	TELEPERM XP
TXS	TELEPERM XS
USB	Universal Serial Bus
VDU	video display unit
VFD	variable frequency drive
V&V	verification and validation
VVER	Vodo-Vodyanoi Energetichesky Reactor (*Водо-водяной энергетический реактор)*
WAN	wide area network
WDM	wavelength division multiplexing
WDPF-II	Westinghouse Distributed Processing Family

1. INTRODUCTION

Oak Ridge National Laboratory (ORNL) has been engaged by the U.S. Nuclear Regulatory Commission (NRC) Office of Nuclear Regulatory Research (RES) to perform research to be used in the development of review guidance and associated acceptance criteria for use by regulatory staff in confirming that highly integrated control room (HICR) designs are in conformance with NRC requirements. The principal features of the HICR are extensive use of multipoint access digital network communications and video display intensive operator workstations. These features provide operations flexibility and potentially increase operations and maintenance efficiency. However, new failure modes are possible that must be considered. The preference of both NRC and the commercial nuclear power industry is that guidance be provided that would minimize detailed open-ended, case-by-case reviews of every system. The purpose of this report is to document technical information used in the development of guidance that specifically addresses issues related to networked communications between safety divisions and between safety-related equipment and equipment that is not safety related. This report is intended to provide clarification of the acceptance criteria for networked communications and workstations involving safety systems in recognition of the inherent differences between modern digital-communication-based systems and hardwired analog systems that have been used in the past. Note that recommended guidance is not necessarily applicable to interactions among entities that are within the same safety division or that involve only nonsafety systems.

1.1 Research Approach and Scope of Guidance

The three components needed to establish detailed technical basis for regulatory guidance are (1) operating experience and lessons learned, (2) accepted consensus practices, and (3) analysis of possible failure mechanisms. For this research, the information required to take the first step—review applicable operating experience relative to digital workstations and network communications—has been drawn principally from several international power reactors as the United States has comparatively less experience with digital communications implementation in nuclear power plant (NPP) safety systems. Industry standards from the Institute of Electronic and Electrical Engineers (IEEE), International Electrotechnical Commission (IEC), and others including non-nuclear consensus documents have been reviewed as a part of determining accepted consensus practices—the second step. In the third step, digital network communication failures were studied, especially examining architectures that apply to nuclear safety systems. A taxonomy of error types, message types, and failure mechanisms was created.

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

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

This report provides the following information:

1. communications types and structures used in a representative set of international nuclear power reactors and I&C communication functions that are addressed in this report . These include
   - communication among safety divisions,
   - communications from safety divisions to nonsafety systems,
   - communication to safety equipment from a nonsafety workstation, and
   - connection of nonsafety programming, maintenance, and test equipment to safety divisions.
2. communications issues derived from standards and other source documents relevant to safety and nonsafety communications.

Improper communications within a safety division could compromise the safety function. However, such intradivisional communication is addressed by existing regulatory guidance.

10 CFR Part 50, Appendix A (Criterion 24, 25, and 29) and IEEE 603 (Sects. 5.6.3.3 and 6.3.1) require that the safety system provide the safety function in the event of any single failure. Nonsafety systems, which are not directly regulated, can exhibit multiple failures. Improper communications in a nonsafety system could conceivably place the plant in an unanalyzed condition. This report, however, addresses only communication that is sent to or received by safety systems.

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

This report presents the findings and observations obtained in the course of the associated research and does not indicate NRC endorsement of the designs and methods reported. The Foreword to this report provides additional information concerning this subject.

1.2 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 some nonsafety 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 may 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.

*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 Protection System/Safety Automation System (PS/SAS). See Sect. 3.10 for a more detailed description.

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 component 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 NRC Information Notice 93-57 (Ref. 1). 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, 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 failure 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.

A more recent communications event, described in NRC Information Notice 2007-15 (Ref. 2), involves failure of variable frequency drive (VFD) controllers on boiling water reactor (BWR) recirculation pumps at Browns Ferry (BF) Nuclear Station, Unit 3. Controller failure was apparently caused by excessive network traffic (i.e., a data storm) on the plant integrated computer system (ICS) Ethernet network. The controllers were determined to be susceptible to lock-up and delayed response failures because of data storm as determined by on-site testing and consultation with the equipment vendor. Licensee corrective actions included (1) developing a network firewall device that limits the connections and traffic to any potentially susceptible devices on the plant ICS network and (2) installing a network firewall device on each unit's VFD controller and condensate demineralizer controller. Note that although only nonsafety-related network devices became nonresponsive during this incident, it is important to protect both safety-related and nonsafety-related devices on the plant network to ensure the safe operation of the plant. The transient on August 19, 2006, unnecessarily challenged the plant safety systems and placed the plant in a potentially unstable high-power, low-flow condition. The potential safety implications for future similar events would depend on the type of devices that are connected to the plant Ethernet.

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.

1.3 Operator Interface and Communication Structures

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 NPP's defensive measures is required to be independent. 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; display of this data 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 operator interface and information display guidelines arise from prior experience with communication systems and the safety and control requirements of NPPs.

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.

Data Pedigree—The pedigree (i.e., the history and validity) of information presented to plant operators must be ensured. During the data networking and signal processing, data may be delayed or corrupted.

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.

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.

Typical digital communication concepts that are components of the I&C architectures under consideration are shown in Fig. 1.1. One illustration (a) shows communication between a nonsafety system and a safety system via a dedicated, point-to-point communication link. The other (b) shows communication between nonsafety system(s) and a safety system via a multi-point network. 1.2 shows a simplified generic I&C architecture for sending safety system information to multidivisional display stations in the control room.

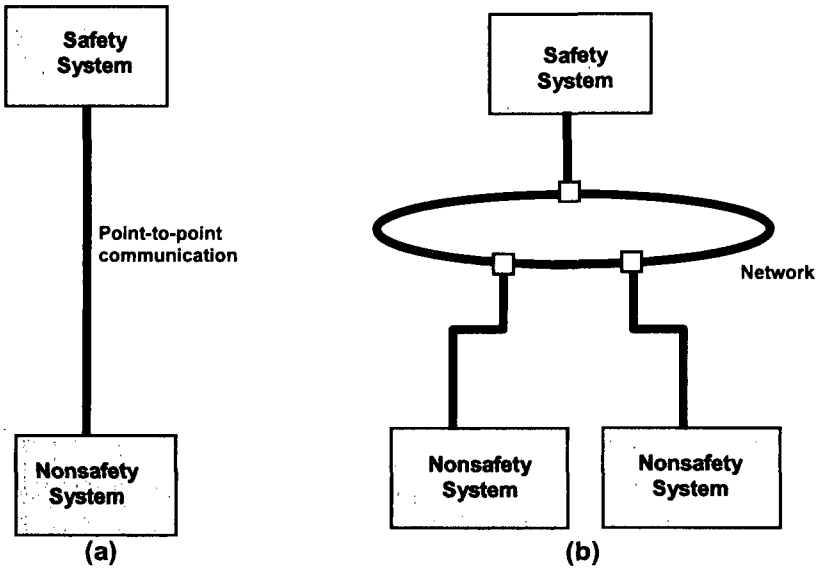

Fig. 1.1. Typical communication structures within the scope of this document.

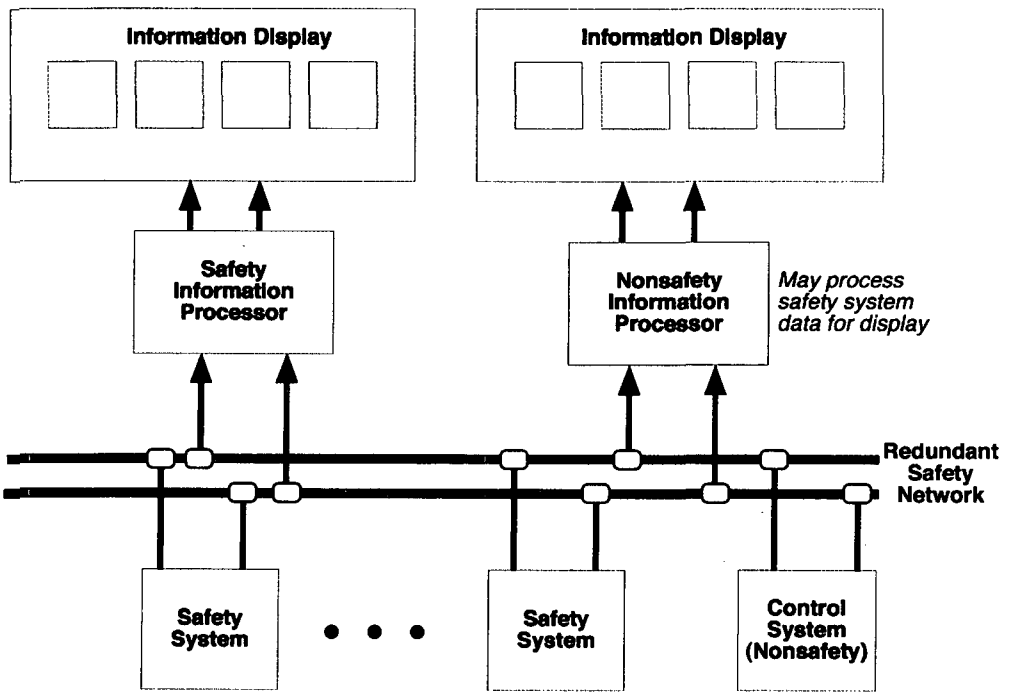

Fig. 1.2. Simplified generic I&C architecture for sending safety system information to multidivisional display stations.

1.4 Report Organization

Many chapters can be written on the 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 five major sections: communication vulnerabilities,

international nuclear plant experience, consensus practices, key issues for communication security and reliability, and evaluation methodologies. Background information on communication architecture, 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 Station Review," describes digital communications at six different international nuclear power 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. "Equipment Qualification and Communication Security" discusses cybersecurity and equipment qualification. The "Structured Methodology for Evaluation of Communications" section describes a review philosophy and lists acceptance criteria for interdivisional safety communications and nonsafety-to-safety communications. Appendixes provide additional information on the communication-specific criteria excerpted from the *Code of Federal Regulations*, Open System Interconnection (OSI) seven-layer model, multiplexing, triggers for communication errors, NRC endorsements, network timing, with additional review information from non-nuclear standards (two appendixes), and the Byzantine Generals' Problem.

2. COMMUNICATION VULNERABILITIES

Communications networks that connect safety-grade systems to other safety-grade systems will be safety grade themselves. Network devices that are designed to be physical and logical isolators are used for any connections to safety systems (e.g., safety-to-safety and nonsafety-to-safety). The portions of the network designed for safety use and the isolator are designed to safety criteria. 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*). The single-failure criterion only applies to safety-grade equipment; nonsafety equipment is presumed to have unrestricted and unlimited failure. A single failure is in the safety-grade isolator and must accommodate any failure or combination of failures in the nonsafety-grade connected network. Therefore, the only credible failure of the safety isolator is disconnection from the nonsafety network. Further, properly isolated safety systems must be designed to perform their designated protection function in the presence of fault or failures in the network isolation device.

This section provides background information on the fundamentals of communications and communication error 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, which has the potential to be received, acted on, and to generate incorrect actions. 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 Generalized Structure of NPP Safety Communications

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. 2.1. 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 whether a module can put information on the bus. A motherboard may have several buses. A number of older standards exist such as IEEE 796 (Ref. 3) 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.

---

*See Appendix A of this report for applicable excerpts from 10 CFR Part 50, Appendix A.

†Vulnerability as it is used in this section refers to susceptibility to communication failure or error, not to security-related exposure.

‡A loss of communication can be partial or intermittent; sufficient delay can be considered either lost or corrupted.

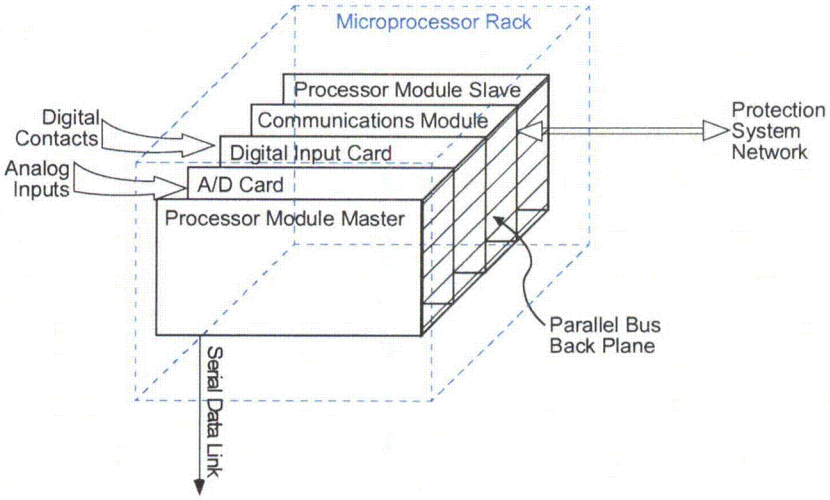

Fig. 2.1. Generic microprocessor-based rack.

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 to compromising the safety function 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 the 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.

2.2 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,

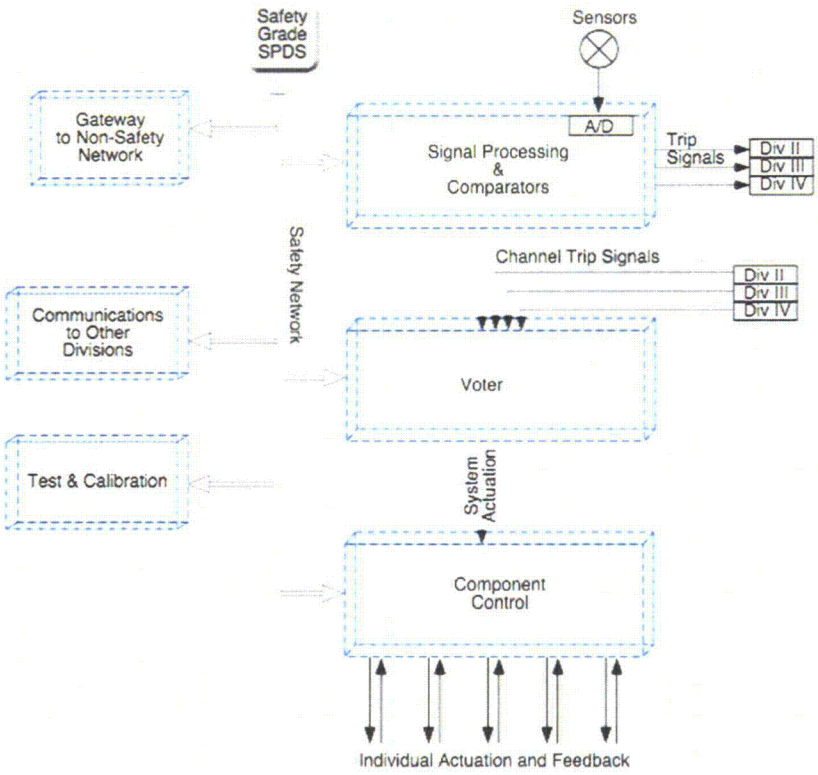

Fig. 2.2. A representative arrangement of modules in a digital protection system.

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 a 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.

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.

2.2 Communication Network Architecture Context

2.2.1 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. 2.3. Appendix B contains further description of the layers. The lower protocol layers, especially the lower four layers, are responsible for reliable message transmission and operate independently of the applications. The upper layers are more devoted to users' applications and use the reliable transportation services supplied by the lower layers.

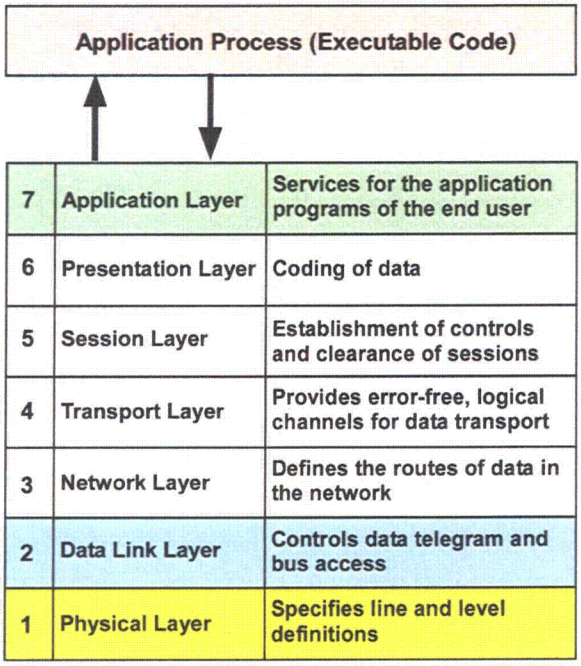

Fig. 2.3. OSI model layers and their relation to executable code.

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.

*Note that 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. Similarly, not every protocol provides or needs all seven layers.

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 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. Protocols at succeeding lower levels of the OSI model encapsulate data coming down from higher levels with information that the lower level protocols need to perform their functions. To maintain independence between OSI layers, no protocol is supposed to make assumptions about or use data in part of the message except the encapsulation that it does itself.

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 B). 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.

New NPPs (Generation III+) and upgrades to existing plants 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 receivers.

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.

A network, for example, 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. 2.4.

2.2.2 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 NPP 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 and otherwise constrained instrumentation networks typically used in safety-critical, high-integrity communication, only layers one, two, and seven of Fig. 2.3 are utilized. Some of the lower layers functions (1–6) can be handled at the application layer (7) using application-specific methods. Systems

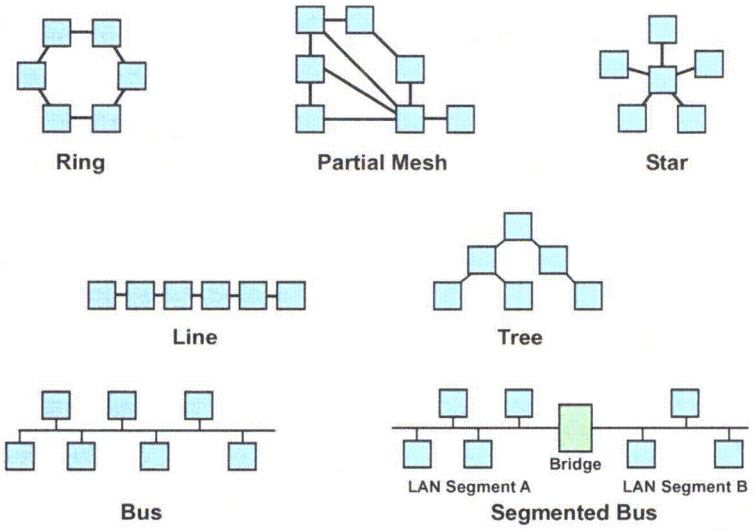

Fig. 2.4. Typical communications network topologies.

conforming to an established protocol (like PROFIBUS) are more likely to have application-independent layers of software (communication stacks) and hardware [application-specific integrated circuits (ASICs)].

The reduced layer model is shown applied to a safety system in Fig. 2.5. This example also illustrates the use of a gateway bridging different communication protocols and the use of a repeater.

The selection of network topology for an application is determined on the basis not only of the communications paths needed, 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 in the event of a link failure,
2. fault detection through the comparison of transmissions received through multiple links, and
3. fault removal by automatically reconfiguring transmission paths around failed links.

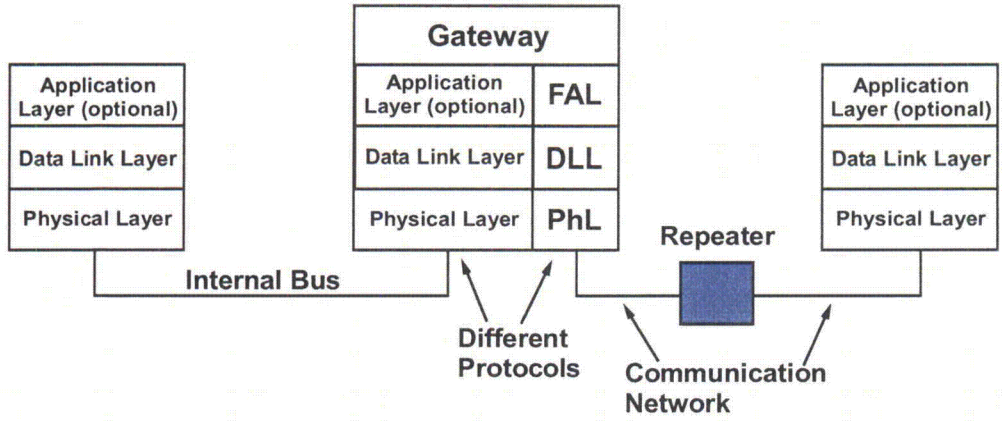

Fig. 2.5. Example of three-layer model applied to a safety system network. Gateway and repeater are present as example network features. (Adapted from IEC 61784; see Ref 41).

*Design of digital communication networks for industrial applications is strongly influenced by factors in economic considerations.

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.

Redundant topology examples are shown in Fig. 2.6. Further information on network redundancy is available in Refs. 4 and 5. A good but dated safety system data communications reference is also available in NUREG/CR-6082 (Ref. 6).

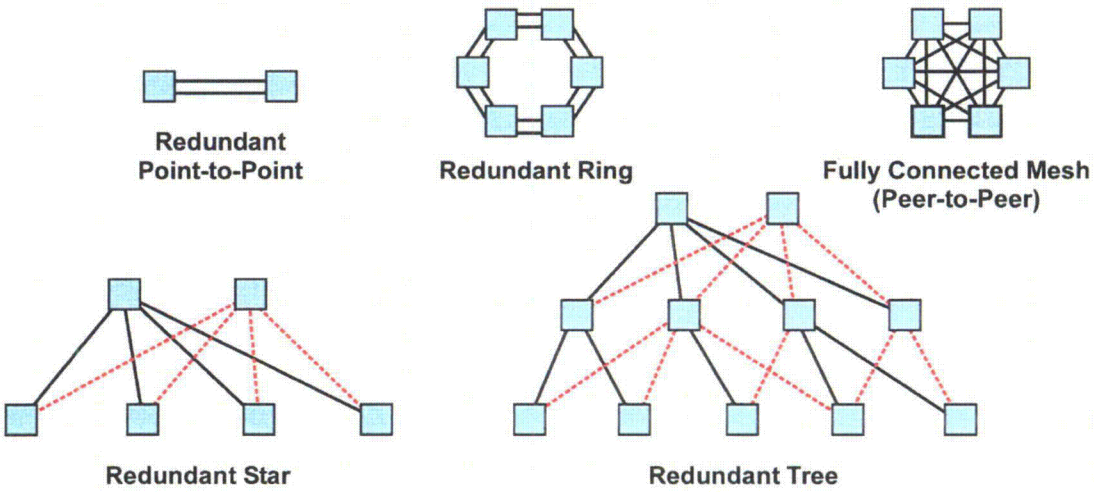

Fig. 2.6. Communication networks with redundant topological features applicable to safety.

The use of redundancy is quite common in critical systems. Although an N-modular redundant system requires more hardware and increases the risk of introducing the Byzantine Generals' Problem, the redundancy can greatly increase the reliability of the system compared to its simple point-to-point counterpart. Redundancy or backup mechanisms will enhance the reliability of a system. Redundant elements support a fault-tolerant architecture. That is, unlike the point-to-point architecture, a redundant system can withstand the failure of one (or more) element, and the system is still capable of performing its required function.

The fundamental idea behind N-modular redundancy is that of parallel reliability. These systems can also compensate for correctness issues stemming from faults injected during the design and specification phases of a project. The independent modules all perform the same task in parallel and then use some voting scheme to determine what the correct answer is. This voting overhead means that N-modular redundant systems can only approach the theoretical limit of reliability for a fully parallel reliable system.

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 reliability might be compromised. Nonconstant topologies make comprehensive testing very difficult.

The National Research Council (Ref. 7) 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. Multinode networks can be made as robust and perhaps more so than point-to-point topology through fault detection and handling, access management, and other features; however, the complexity and concomitant effort to analyze potential failure modes increases with nodes on a network. Whatever topologies become

implemented, whether bus or point-to-point, they need to be designed to ensure performance, reliability, and failure states within the design basis requirements of the protective system.

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 being sent information that indicates, for example, a unique serial number, class identifier, a recipient identifier, the time of origination, the sender identifier, and a corruption detection key. Other information may also be added by routers along the network. Several of the standards discussed in Sect. 4 go into detail as to preferred protocols for message construction.

2.2.3 Multiplexing

Multiplexing is the process of sending more than one data stream simultaneously over a communication channel (transmission medium) where multiple message signals or data streams share the same resources (time, frequency, and space) without interfering with each other. The main goal of multi-access network protocols is to combine many data streams on a smaller number of data paths. The most common multiplexing techniques are time division multiplexing (TDM), wavelength division multiplexing (WDM), statistical multiplexing, and packet multiplexing. These techniques were evolved for the need to transmit many channels of voice or data simultaneously mainly for voice communications in public switched telephone network (PSTN) and data transmission for computer networks. A multiplexing technique may be further extended into amultiple access method, for example TDM into time-division multiple access (TDMA) and statistical multiplexing into carrier sense multiple access (CSMA). A multiple access method makes it possible for several transmitters connected to the same physical medium to share its capacity. Multiplexing is provided by the physical layer of the OSI seven-layer model. Additional details regarding multiplexing are included in Appendix C.

The users (i.e., transmitting nodes) are not coordinated in asynchronous network communications. Thus, the resultant signal at the receiving nodes is the summation of incoming signals, arbitrarily delayed from each other. In synchronous network communications, there is a known time difference between two incoming signals to the receiver. Packet transmission is asynchronous in nature. Deterministic networks may be either synchronous or asynchronous.

2.3 General Nature of Digital Communication Errors

Communication is fundamentally about the successful transmission and reception of information from a source to one or more receivers. By extension, this communication can include the delivery of a response from the receiver(s) to the source, showing how the information was received and used. When all goes well with a communication event (i.e., no bandwidth limitations, noise, transients, component faults, and errors), information is correctly assembled and coded at the source then transmitted to the receiver; at the receiver, that information is decoded and used correctly. For a variety of reasons and from myriad sources, failures and errors can appear in numerous places along the path from source to receiver. Possible error points of origin include the following:

1. source-generated errors,
2. communication/transmission-channel-generated errors (including interposed bridges and routers),
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 marginalizing its usefulness. Transmission failure refers to a loss of information or sustained delay so that no message is received. A general requirement for NPP safety

systems is for interdivisional data communication or nonsafety–to-safety communication, no condition or event related to external communications should alter execution of the safety function. This requirement includes communication network events such as loss of data and abnormal plant events. These two classes of communication failure form the basis of an evaluation methodology for interdivisional communications and nonsafety-to-safety communications. The methodology is discussed in Sect. 6.

2.3.1 Error Types

In communication systems, desired information is estimated from the known received signal. The sent signal must be estimated from the received signal on the basis of whatever information is available from knowledge of the sending source and process and from redundancies in the signal itself. Although the transmitted signal is generated from a finite and deterministic signal set, the received signal is stochastic because the influence of noise, interference, and transmission errors is random. Thus, the performance of the communication system has a random component. As a result, the inherent nature of the estimated error is random, and the error is often measured as "on-average" error. (Note that the instantaneous error of a particular case may vary with the error expected of the communication systems.)

A nonexhaustive list of communication error types has been compiled from several sources (Refs. 8 and 9). The errors are divided into three categories (derived from the four sources listed above by treating sender and receiver together) according to whether the error is predominantly communication channel related, associated more with the transceiver (transmitter and receiver), or a result of network segmentation. These error types also include the failure modes that the National Research Council (Ref. 7) considered associated with digital communication systems.* The National Research Council report also suggested considering failure modes associated with shared resources such as multiplexers. (See also Appendix D for a list of triggers for communications errors.)

The first category of error types 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
Babbling Idiot (Commission Fault)
Inconsistency (Byzantine Generals' Problem)
Excessive Jitter
Collision

*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)."

Corruption—Messages may be corrupted because of errors in communications processors, errors introduced in buffer interfaces, errors introduced in the transmission media, from interference, or simply inherent error called additive white Gaussian noise (AWGN). The occurrence of message errors during transmission is a common event for standard communication systems. Due to the typical electronics, once a communications protocol such as modulation is selected for signal transmission, there is a fixed average error rate associated with that protocol. In other words, if, for example, the selected modulation scheme is binary phase shift keying (BPSK), the bit-error probability is known: the average probability of bit error is 10^{-5} for the received signal-to-noise ratio (SNR) of 9.6 dB. To improve on this performance, often some form of error detection or correction technique such as cyclic redundancy checks (CRCs) is applied.* CRCs offer a high probability of error detection in receivers. More powerful bit-error correction codes such as a convolutional code can be used to correct some of the erroneous detected bits. A protocol involving retransmission of packets such as automatic repeat request (ARQ) is another way to improve transmission performance. The combination of these modulations, error correction coding, and retransmission combined with other techniques such as diversities in the system can offer a communications system with very low or near-zero probability of bit error. 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. All these processes for correctly receiving a message result in processing delay. If the combined effect of the processing delay including repeat and transmission delay takes longer than a specified deadline, a message is considered as "Unacceptable Delay." In the preceding discussion, it is presumed that network design procedures have matched the sender and receiver protocols; otherwise, communication would either not occur or results would be erratic with resultant data corruption.

Unintended Repetition—Messages (old and not updated) 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. To reduce the average probability of message loss, redundancy can be used to send the same message multiple times (time diversity) or to send the message by multiple routes (path or space diversity). Depending on the transmission medium, protocol, and application, general communication systems use many forms of diversity, including time, frequency, space, polarization, code, or combinations of these basic diversities. Message repetition is an example of the time diversity; mesh network is a form of space diversity; most of the current communications systems use code diversity.

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. Communications systems may contain a depository that stores messages (e.g., FIFO in switches, bridges, routers) or may use protocols that change the sequence depending on the priority. Multiple sequences from various sources or reports relating to different object types are appended to a message frame before transmitting. Upon reception, these sequences are monitored separately, and thus, errors can be detected. The average error probability of Incorrect Sequence detection should be insignificant compared to the average probability of error for the real message.

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

Unacceptable Delay—Messages may be delayed beyond their permitted arrival time window. Conditions leading to delays include complexity of the signal recovery, congested transmission medium, interference, service delay, and delay in sending buffered messages. A benefit of advanced signal

*A CRC takes a data stream as input and produces a fixed-length output value. CRCs are especially effective at detecting common errors caused by transmission channel noise.

processing techniques (CRC or other forms of error correction, diversity, and retransmission), is correct message reception despite corruption by noise, channel faults, or interference. However, the time cost is delay in message reception. Consider the following example: message errors may be recovered in three possible scenarios: (a) immediate retransmission, (b) retransmission using spare time at the end of the cycle, or (c) treat the message as lost and wait for the next cycle to receive the next value. In case (a), all the messages are slightly delayed. In case (b) only the retransmission message is delayed. Both cases may be generally considered as an Unacceptable Delay. Case (c) would be considered as an Unacceptable Delay unless the cycle retransmission interval is short enough to ensure that delays between cycles are not significant and the next cycle value can be accepted as a replacement for the missed previous value.

Insertion—Messages may be inserted into the communication medium from unexpected or unknown sources. These messages, also known as interference, 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 not be 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 (Ref. 2).

Babbling Idiot (Commission Fault)—A node that sends messages at arbitrary points in time exhibits the most serious failure in a distributed system based on a broadcast bus (Refs. 10–12). Nodes that are affected by this kind of failure mode are called Babbling Idiots. Babbling Idiots send messages without obeying the bus access rules imposed by the bus access methodology, thus corrupting the messages being transmitted by the nonfaulty nodes. It has long been a criticism of event-triggered systems that they are unable to detect or tolerate Babbling Idiot Failures or Commission Faults. A commission failure occurs if a process (or node) produces a result (or message, event, etc.) when none should have been produced. In a real-time system, this extends to an event that repeatedly occurs too early. The Babbling Idiot Error is distinct from the Broadcast Storm because the former is the result of one malfunctioning node, whereas the latter is the mounting propagation of responses from multiple nodes. The Babbling Idiot Failure results in a process/node consuming more resources than it would normally use. For example, consider a set of nodes communicating through a shared bus; if one node suffers a Babbling Idiot Failure and begins to transmit extra messages onto the bus, then it may starve the other correct nodes on the bus of network bandwidth. The Babbling Idiot Failure is applicable to both deterministic and nondeterministic networks.

*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 that are not part of that tree, leaving a single active path between any two network nodes.

Inconsistency (Byzantine Generals' Failure)—The inconsistency error is often referred to as a Byzantine Fault, which is a fault presenting different symptoms to different observers. Correspondingly, a Byzantine Failure is the loss of a system service due to a Byzantine Fault in systems that require consensus (Ref. 13). The Byzantine Generals' problem arises when a single failure propagates via the cooperative mechanisms that the N-modular redundant (NMR) system uses and causes the failure of the entire NMR system. The literature suggests that the triggers of Byzantine Generals' Faults are extremely difficult to anticipate so the best solution is to devise ways to handle the situations they would create should they happen (Ref. 14). The only way that Byzantine Generals' Failures cannot happen in a system is if there is no cooperation among redundant elements. For example, many distributed systems have an implied system-level consensus requirement such as a mutual clock synchronization service. Failure of this service will bring the complete system down. Asynchronous approaches do not remove these problems. Any coordinated system actions will still require consensus agreement. If the system cannot be designed such that a consensus is not needed, the system must be designed to prevent the fault from propagating. However, other than using intrinsically reliable circuit components, the only way for implementing a reliable computer system is to use several different "processors" to compute the same result and perform a majority vote on their outputs to obtain a single value. (The voting may be performed within the system or externally by the users of the output.)

Excessive Jitter—The jitter is cycle-to-cycle time variation observed when a computed result is output to the external environment. Jitter is a form of delay in which the delays are small but variable; hence, jitter is usually not placed in the same classification as Unacceptable Delay. Problems with jitter show up in tight feedback timing loops such as would be associated with real-time controllers or in data acquisition systems. Jitter can come from variations in time responses and latencies of a communication channel, which includes transceivers as well as media. Message packets that are passed through multiple nodes, gateways, and routers accumulate delay and delay variability. Network jitter problems complicate synchronization among packets from a single media stream. In nondeterministic networks, packet collision interference contributes to variability. Jitter buffers can be used to alleviate the jitter effect, although such buffers will add fixed delay to the system.

Collision—In nondeterministic networks, such as Ethernet, multiple devices may attempt to transmit data at exactly the same time, resulting in a collision. Collisions are a natural occurrence on Ethernet networks. Ethernet uses Carrier Sense Multiple Access/ Collision Detect (CSMA/CD) as a method of allowing devices to schedule transmission using the signal carrier line. The CSMA/CD operates at the physical layer in the OSI seven layer model (see Sect. 2.2.1). However, even with collision detection protocols, two devices can simultaneously transmit and subsequently collide. The network detects the collision of the two transmitted packets and discards them both. The result of such collision is decreased network efficiency (variable transmit times) and potentially corrupted data such as truncated packets. The possibility exists that error checking protocols may not identify an error resulting from a collision and therefore pass corrupted data to a receiver. For these reasons, nondeterministic networks are not recommended for safety-grade networking. Nondeterministic networks such as Tokin Ring never have collision issues because the information packets only travel in one direction, and all network nodes communicate so as to know when information is being passed forward—each node communicates via a token.

The second category of error types is more closely associated with source and receiver function as shown in 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
Message Too Early
Encoding/Decoding

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.

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.

Message Too Early—An application program can release a message prior to its specified scheduled time. This release may be due to a priority inversion or an out-of-synchronization clock at the sending system. Generally, the communication layers are not responsible for timed release of messages held in a queue; that is the task of the application program and thus may be more of a software design issue. The early message is likely sent in earnest with the expectation that it be received and acted on. It, however, may be subsequently rejected by the receiver(s). For that reason, this error type must be considered in the overall design of the communication system.

Encoding/Decoding—Messages may be incorrectly encoded at the transmitter or decoded by the receiver. The exact encoding/decoding protocols must be used by sender and receiver(s). A mismatch of this level of protocol typically will result in nonperformance; however, two closely related protocols or variations on a protocol could produce erroneous data and inconsistent operation.

The third error category applies to networks that are segmented (i.e., they contain bridges or routers). These error types are shown in Table 2.3.

Table 2.3. Segmented network-related errors

Very Long Delays in Bridges and Routers
Very Long Times to Initiate Communications
Complete Blockage

Very Long Delays in Bridges and Routers—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.

Very Long Times to Initiate Communications—Similar to delays incurred by routers, switches, and bridges, two devices attempting to communicate may experience delays in establishing authentication across segmented networks.

Complete Blockage—Several conditions such as time-out, re-initialization, and hardware failure can result in bridges, routers, and switches being out of service for an indefinite period. This design issue must be evaluated if bridges, routers, or switches 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 2.4. 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 2.4. Relationship of communication error types with the three primary abstraction layers

Error category	Communication layer interaction[a]		
	Physical interface *Layer 1*	**Data link** *Layer 2*	**Application** *Layer 7*
Corruption	Corruption within the physical media or interface components	Handles or introduces corruption	Message handling flaw can result in corruption
Unintended Repetition		Handles or introduces Unintended Repetition	Applications might send message >1 time due to flaw
Incorrect Sequence		Handles or introduces Incorrect Sequences	Applications might have responsibility for sending some types of messages first
Loss (Deletion)	Loss within the physical media	Flaw could cause loss	Flaw could cause loss
Unacceptable Delay	Flaw could cause delay	Flaw could cause delay	Flaw could cause delay
Insertion	Flaw could cause Insertion	Flaw could cause Insertion	
Masquerade	Flaw could cause Masquerade	Flaw could cause Masquerade	
Incorrect Addressing	Connected to the incorrect destination[b]	Sends the message on the wrong communication port[c]	Applications can be responsible for node names that are ultimately translated into network addresses
Broadcast Storm		Incorrect implementation of Spanning Tree Protocol (or Equivalent) can result in Broadcast Storm	Repeated response by application to same message circulating on a network can result in Broadcast Storm
Babbling Idiot (Commission Fault)	Failed components at the physical interface can cause commission faults		
Byzantine General (Inconsistency)			Application may fail to handle a Byzantine Generals' Failure
Excessive Jitter	Noise or faulty components		
Collision	Attempts to control collisions	Handles incorrect message potentially resulting from collision	

Table 2.4. (continued)

Error category	Communication layer interaction[a]		
	Physical interface *Layer 1*	**Data link** *Layer 2*	**Application** *Layer 7*
Buffer Overflow	Hardware buffer can overflow	Memory Buffer Overflow	Memory Buffer Overflow
Data Out of Range			Application creates data value inconsistent with specification
Incorrect Ordering		Interchange of data could occur at the data link layer	Application layer can incorrectly assemble message components
Message Too Early		Possible timing clock error	Application can send message before designated time
Encoding/Decoding	Protocols must match		
Very Long Delays in Bridges and Routers	Holdup up in routers and bridges possible because of internal processing speeds		
Complete Blockage	Similar to Very Long Delay (above)		
Very Long Times to Initiate Communications Through Bridges and Routers	Latency in authentication can delay initiation		

[a]See Fig. 2.1.

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

[c]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.

Several defenses against communication errors are recognized and described in the literature. Table 2.5 matches 16 defensive measures with the error types described in the previous paragraphs. The table is for reference and should not be considered exhaustive of the possible corrective and mitigation strategies available. A brief description of the defense methods is given in Table 2.6.

Many of these defense methods are taken from EN 50159-2 (Ref. 15).

2.3.2 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 usage. Six categories of message types are shown in Table 2.7. These data types are described in the subsequent paragraphs.

Table 2.5. Matching of error with possible defense methods

Error	Defense															
	Sequence number	Timestamp	Time out	Source and destination identifier	Feedback message (acknowledgements)	Identification Procedure	Safety code (CRC)	Cryptographic techniques	Redundancy (replication)	Membership control	Atomic broadcast	Apply time-triggered architecture	Apply bus guardian	Prioritization of messages	Inhibit times	Hamming distance applied to node addresses or message identifiers
Corruption					•		•	•	•							
Unintended Repetition	•	•							•			•	•		•	
Incorrect Sequence	•	•							•			•				
Loss (Deletion)	•		•		•				•			•				
Unacceptable Delay		•	•		•							•		•	•	
Insertion	•			•	•	•	•[a]		•							•
Masquerade					•	•	•[a]	•								•
Incorrect Addressing				•												
Broadcast Storm													•			
Babbling Idiot													•			
Inconsistency (Byzantine Generals)										•	•					
Excessive Jitter		•										•		•	•	
Collision					•		•	•	•			•	•			
Buffer Overflow					•[b]											
Data Out of Range					•[c]											
Incorrect Ordering					•[c]											
Message Too Early		•										•				
Encoding/Decoding				•	•	•	•									
Very Long Bridge/Router Delay		•	•													
Very Long Times to Initiate Communications		•	•													
Complete Blockage	•	•	•									•		•		

[a] Valid, if the CRC calculation includes data that are not in the message itself, but is known by the transmitter and receiver(s) a priori (for example, a message key and an expected send time).

[b] Valid only for local buffer at the interface layer. Buffer memory overflow at higher communications layers or in the application may not be solved by these defenses.

[c] Valid only if feedback is give to sender that data values or order in message are not in specification.

Source: adapted from J. Alanen et al., "Safety of Digital Communications in Machines," VTT Research Notes 2265, October 2004.

Table 2.6. Brief descriptions of error defense methods

Defense method	Description	Used against this error
Sequence number[a]	Each message has a consecutive number. In the simplest case, the message includes a toggle bit.	Repetition, Incorrect Sequence, Deletion, Insertion
Time stamp[a]	Each message has a time code that describes the sending time.	Repetition, Incorrect Sequence, Delay, Jitter, Message Too Early, Very Long Bridge/Router Delay, Very Long Times to Initiate Communication
Timeout (for example, watchdog)[a]	Receiver accepts messages only when they arrive in time or during a predefined time window. Usually exception handling is used to react upon delayed messages.	Deletion, Delay, Very Long Bridge/Router Delay, Very Long Times to Initiate Communication
Source and destination identifier[a]	Each message has a source and/or destination address or other code.	Insertion, Incorrect Addressing
Feedback message (acknowledgments and echoes)	After receiving a message, the module sends a positive or negative acknowledgement, or after receiving a message, the module sends the whole message or a checksum back.	Corruption, Deletion, Insertion, Masquerade, Buffer Overflow, Data Out of Range, Incorrect Ordering
Identification procedure[a]	The members of the network check the identity of the other members prior to the start of the system or prior to the transmission of a specific message. Identity may include, for example, information about software and hardware versions.	Insertion, Masquerade
Safety code (for example, CRC cyclic redundancy check)	The method adds into the message a checking code; also, other types of data consistency checks are available.	Corruption
Cryptographic techniques[a]	Authentication is applied, and cryptographic code is added to the message to protect against malicious attacks.	Corruption, Masquerade
Redundancy (replication)	The messages are transferred periodically even though no changes in values have occurred; a message may be replicated (for example, sent twice with the other message inverted); the communication subsystem may be replicated.	Corruption Repetition, Incorrect Sequence, Deletion, Insertion
Membership control	The members of the network monitor each other and execute exception handling in case of malfunction in one of the members.	Inconsistency
Atomic broadcast[b,c]	Communication protocol with atomic broadcast ensures that all messages are delivered in the same order to all correct processors in the system and all consumers of the data have a consistent view of data (all accept the data, or all reject it).	Inconsistency
Time-triggered architecture	Messages are scheduled in regard to time. The time schedule is often prefixed by the system designer.	Corruption Repetition, Incorrect Sequence, Deletion, Excessive Jitter, Message Too Early

Table 2.6 (continued)

Defense method	Description	Used against this error
Bus guardian	Transmission of messages is controlled by a hardware that opens and closes the access path for the transmitter to the communication media.	Repetition, Broadcast Storm, Babbling Idiot
Prioritization of messages	The messages are prioritized to enable safety-critical messages to access the bus with minimum delay.	Unacceptable Delay, Excessive Jitter
Inhibit times	Similar to bus guardian, but can be implemented by software at the communication subsystem; after transmitting a certain message, that particular message is put in "quarantine" for a given period of time before it can be transmitted again by the particular transmitter.	Repetition, Unacceptable Delay, Excessive Jitter
Hamming distance applied to node addresses or message identifiers	The node addresses or message identifiers are selected so that any single bit failure in the address or in the identifier produces a nonused address or identifier and can thus be noticed by the receivers.	Insertion, Masquerade.

[a]EN 50159-2, "Railway Applications, Communications, Signaling, and Processing Systems," Part 1: Safety-related communication in closed transmission systems, Brussels, European Committee for Electrotechnical Standardization (2001).

[b]D. Agrawal, G. Alonso, A. El Abbadi, and I. Stanoi, Exploiting atomic broadcast in replicated databases. *Proceedings of EuroPar (EuroPar'97)*, number 1300 in Lecture Notes in Computer Science, p. 496–503, Passau, Germany, August 1997.

[c]X. Défago, A. Schiper, and P. Urban, *Totally ordered broadcast and multicast algorithms: A comprehensive survey*, Tech. Rep. DSC/2000/036, Ecole Polytechnique Fédérale de Lausanne, Switzerland, September 2000.

Source: adapted from J. Alanen et al., "Safety of Digital Communications in Machines," VTT Research Notes 2265, October 2004.

Table 2.7. 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 may be necessary to fix bugs, vulnerabilities to communication errors, 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 setpoints 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. All such changes should be implemented with the relevant safety system in bypass. 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. At a NPP this might include instructions to switch from intermediate to power range set points.

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 to 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 2.8. These methods are illustrative only because there are many ways a designer can develop a system.

Table 2.8. 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 communication error or failure 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
Set Points and Parameters	Transfer of new set points or operating parameters to a system. Communication contains analog values such as temperatures, pressures, and filter settings	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 identify authenticity of sending system. Permit set point changes over controlled and limited node network. Transfers should only occur while the system is not credited with performing its safety function
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 identify authenticity of sending system. Limit crucial commands to point-to-point network. Lockouts may prohibit more than one safety node at a time from using the bus

Table 2.8 (continued)

Message type	Description	Communication example	Potential detrimental effect of error	Possible methods to mitigate effect[a]
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 identify 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] (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
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 network. Otherwise, establish a limitation on the number and types of requests that can be issued during specific periods.

Table 2.8 (continued)

Message type	Description	Communication example	Potential detrimental effect of error	Possible methods to mitigate effect[a]
				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. *Source:* R. T. Wood et al., *Advanced Reactor Licensing: Experience with Digital I&C Technology in Evolutionary Plants*, NUREG/CR-6842, April 2004.

2.4 Synthesis of Technical Information to Support Review of Communication Systems

The key configuration and performance aspects of digital communication systems described within this section can be used to support the review process. Specifically, the information presented in this section enables identification, screening, and assessment of capabilities, characteristics, and strategies that ensure high integrity, dependable communication for safety-relevant applications.

A three-step progression provides the necessary framework to utilize this technical information to facilitate the effective review of digital communications. The steps associated with this review process are as follows:

1. identify architecture and network topology used and note the key characteristics,
2. ensure that known vulnerabilities to communication failures and errors have been screened to define a credible set applicable to the architecture, and
3. assess the application of defensive strategies and the implementing techniques to mitigate the credible communication errors.

The suggested review process focuses on a determination of whether the digital communications design under review has systematically considered and effectively resolved the potential vulnerabilities that experience and analysis have shown to be relevant for the chosen network architecture. Guidance is given in Sect. 6 for a structured methodology for evaluating digital communications.

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 (Ref. 16) 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) (Ref. 17) that creates a two-subclass safety class. IAEA Safety Guide 50-C-D (Ref. 18) provides the IAEA safety grading scheme, including providing examples of classification of major NPP systems and components. IAEA Safety Guide NS-G-1.3 (Ref. 19) 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 safety functions other than those called out in the safety requirements for design.

IEC 61226 (Ref. 20) 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 (Ref. 21) 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

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 61226	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		

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. 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 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. 2. The following discussion gives a number of specific examples of digital protection systems in international reactors. The goal is to identify (a) the logical communication structures, (b) the technology involved, (c) the communication segregation strategy for functional diversity, (d) any redundant communication links to reduce 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. These include techniques to ensure that failure rates of individual links are very low and that there is no common cause failure in the communications systems that compromise the function of the safety system.

3.3 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) NNPs. 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 nonmodifiable 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.

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

Year ~ 2007 to present: TELEPERM XS protection system technology; use of 32-bit processors; use of Function Block programming (that is, function diagrams are translated into code using standard code structures and a library of function block modules); code generators along with standardized code structures are used to translate application-specific notation to source code (Ref. 22); use of system networks.

The following are the safety classes used in the N4 I&C architecture (Fig. 3.1) as well as their descriptions:

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.

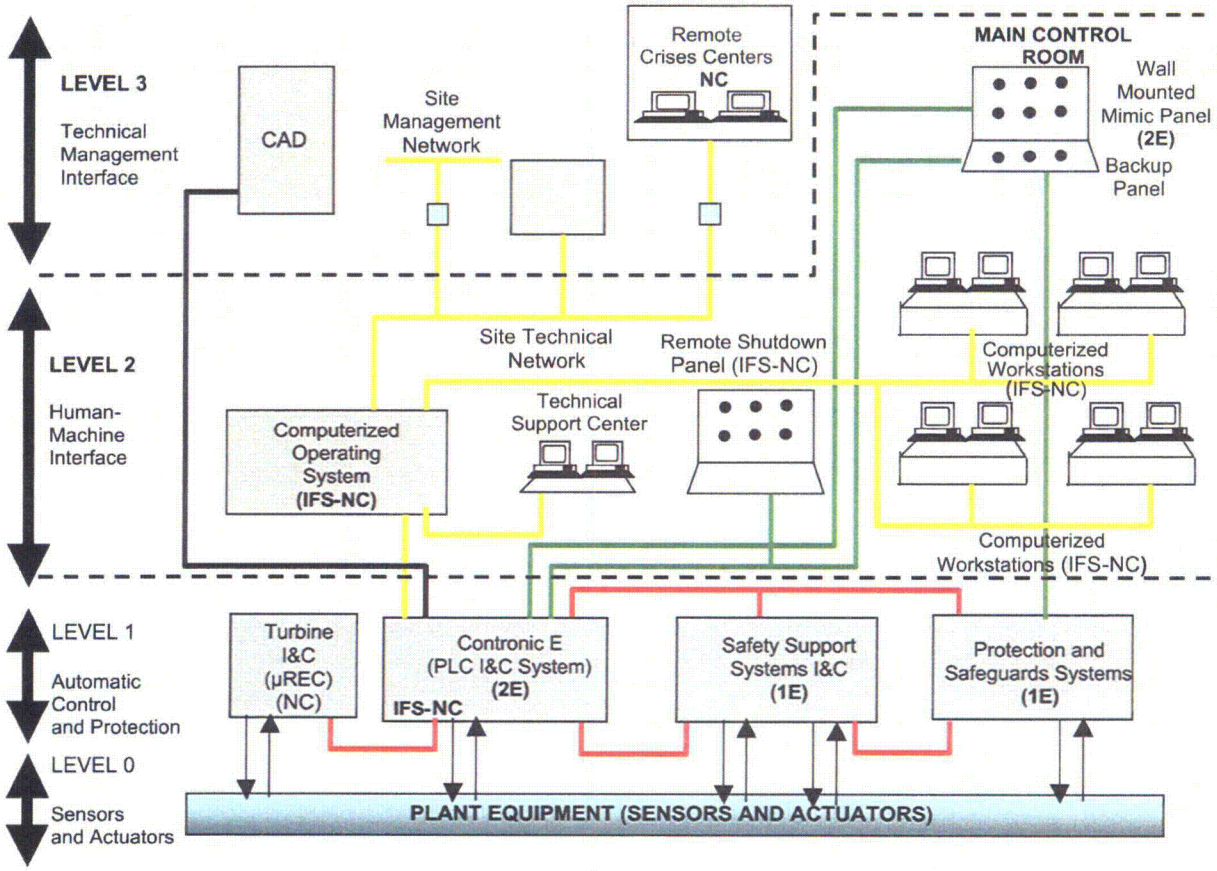

Fig. 3.1. I&C architecture of Chooz B (N4) Plant.

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.

In N4, I&C architecture can be thought of as consisting of four levels or layers from the process to operator, that work together to form an integrated structure. A brief description is as follows (Ref. 23):

Level 0: This is the process layer and consists of the sensors and actuators.

Level 1: This is the automation layer and performs the functions of protection and control. In particular, it provides four main functions as follows: the turbine I&C, the process automation PLC (Contronic E) from Hartman and Braun, safety support I&C which includes an atmospheric steam dump system and control of engineered safety systems, and a protection and safeguards implemented using the SPIN technology.

Level 2: This is the operating and monitoring layer. This layer performs data exchange to/from operators, data storage and retrieval, and information recording. It also includes the main control room panel and remote shutdown panel.

Level 3: This is the (local and remote) technical management level of the plant.

The N4 technology 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 and 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 minutes 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.

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

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.

3.4 Sizewell B (United Kingdom)

Sizewell B is a Westinghouse design PWR that began commercial service in 1995 as the first PWR-style reactor in Great Britain. (See Refs. 24–26.) 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). 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 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 at seven U.S. plants (Sequoyah 1 and 2, Turkey Point 3 and 4, Watts Bar, Diablo Canyon 1 and 2) as well as at the Temelin plant in the Czech Republic. Similar systems were also used at Zion 1 and 2, which are no longer operating. 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. 3.2. 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.

The primary protection system, consisting of the reactor trip system and the engineered safeguards, is illustrated approximately in Fig. 3.3. The figure is the best available in the public domain but lacks sufficient detail to illustrate the network connections. The top-level plant data highway is the Westinghouse WestNet. All sensor data and protection system settings are available in the main control room through the safety network.

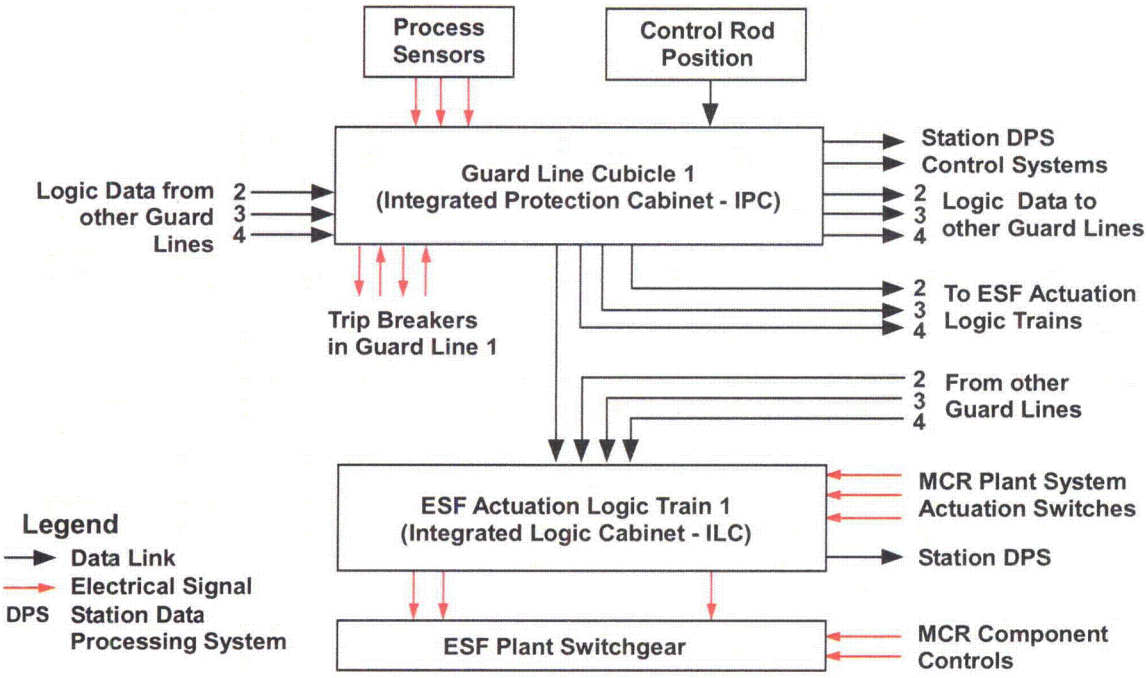

Fig. 3.2. Sizewell B protection system diagram illustrating communications within a division. *Adapted from* G. B. Moutrey and G. Remley, "Sizewell B power station primary protection system design application overview: Electrical and Control Aspects of the Sizewell B PWR," International Conference on 14–15 September 1992, p. 221–231.

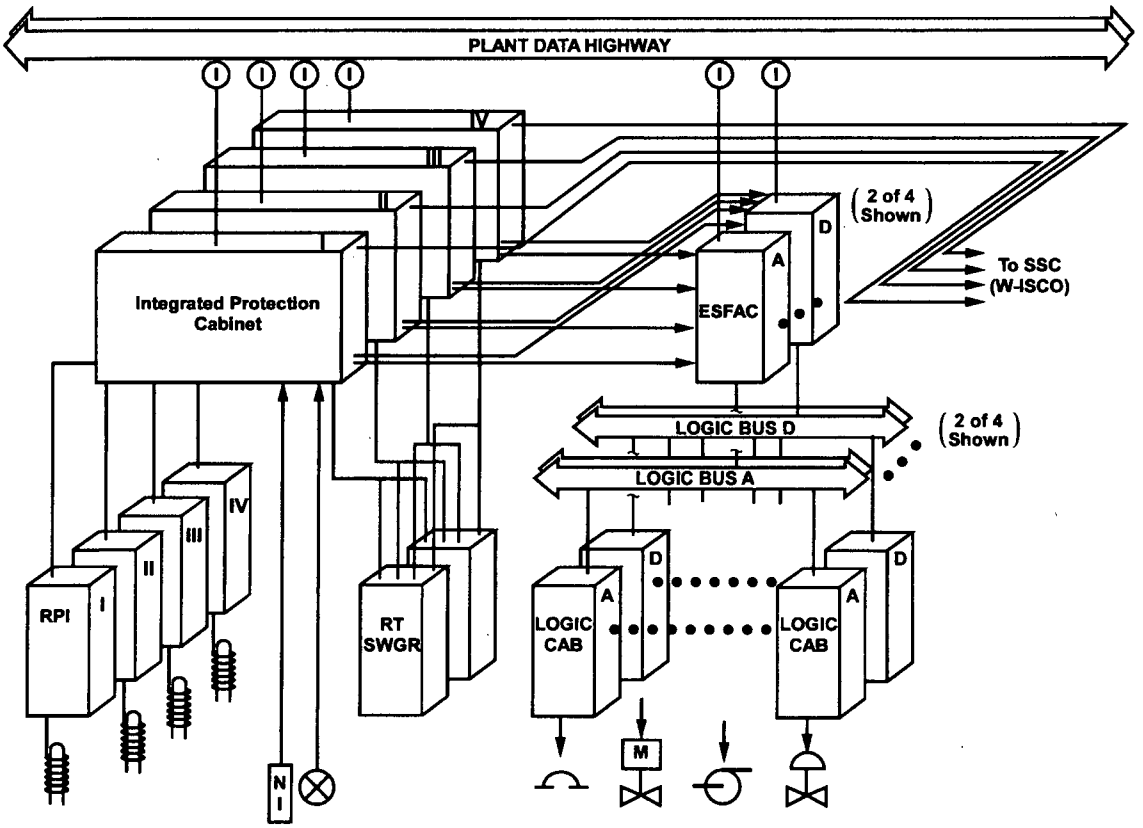

Fig. 3.3. Sizewell B primary protection system. *Adapted from* G. W. Remley, B. M. Cook, and P. A. Loftus, "Sizewell B Integrated Control and Instrumentation System: A Vision Becomes Reality," IEEE 0-7803-0883-2/93.

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. 2.2.

3.5 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. 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. 3.4. 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.

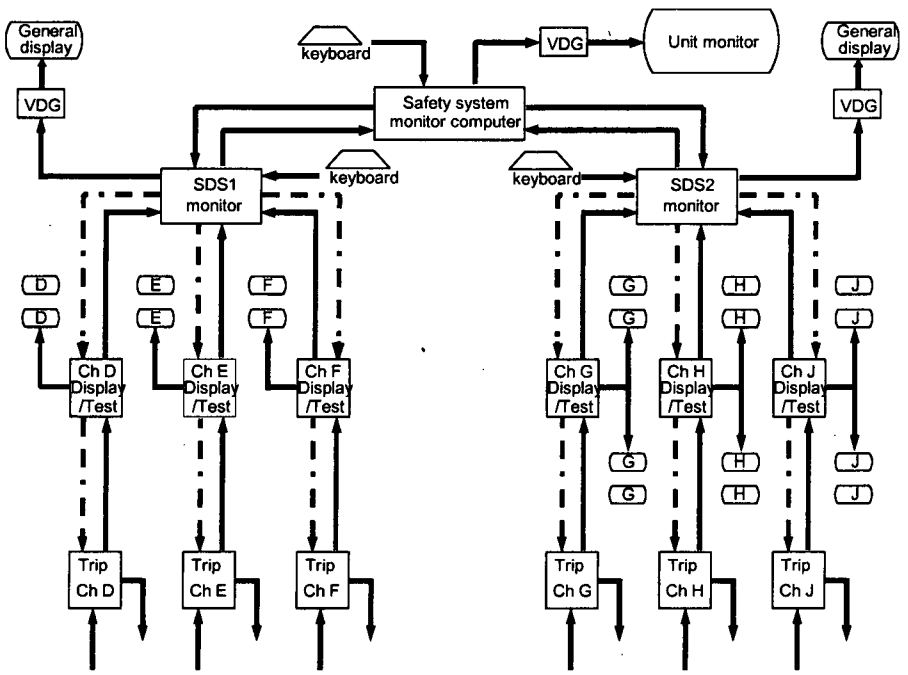

Fig. 3.4. Reactor protection system architecture.

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

3.6 Lungmen Advanced Boiling Water Reactor (Taiwan)

The digital communication technology being deployed at the Lungmen Advanced Boiling Water Reactor (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 (Ref. 27) and the NRC 19th Annual Regulatory Information Conference (Ref. 28).

3.6.1 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 General Electric (GE) NUMAC hardware. Principal features of the RPS communications system (illustrated in Fig. 3.5) are as follows:

- The RPS signal communication from sensors to the digital trip module (DTM) is implemented in a non-networked 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 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.

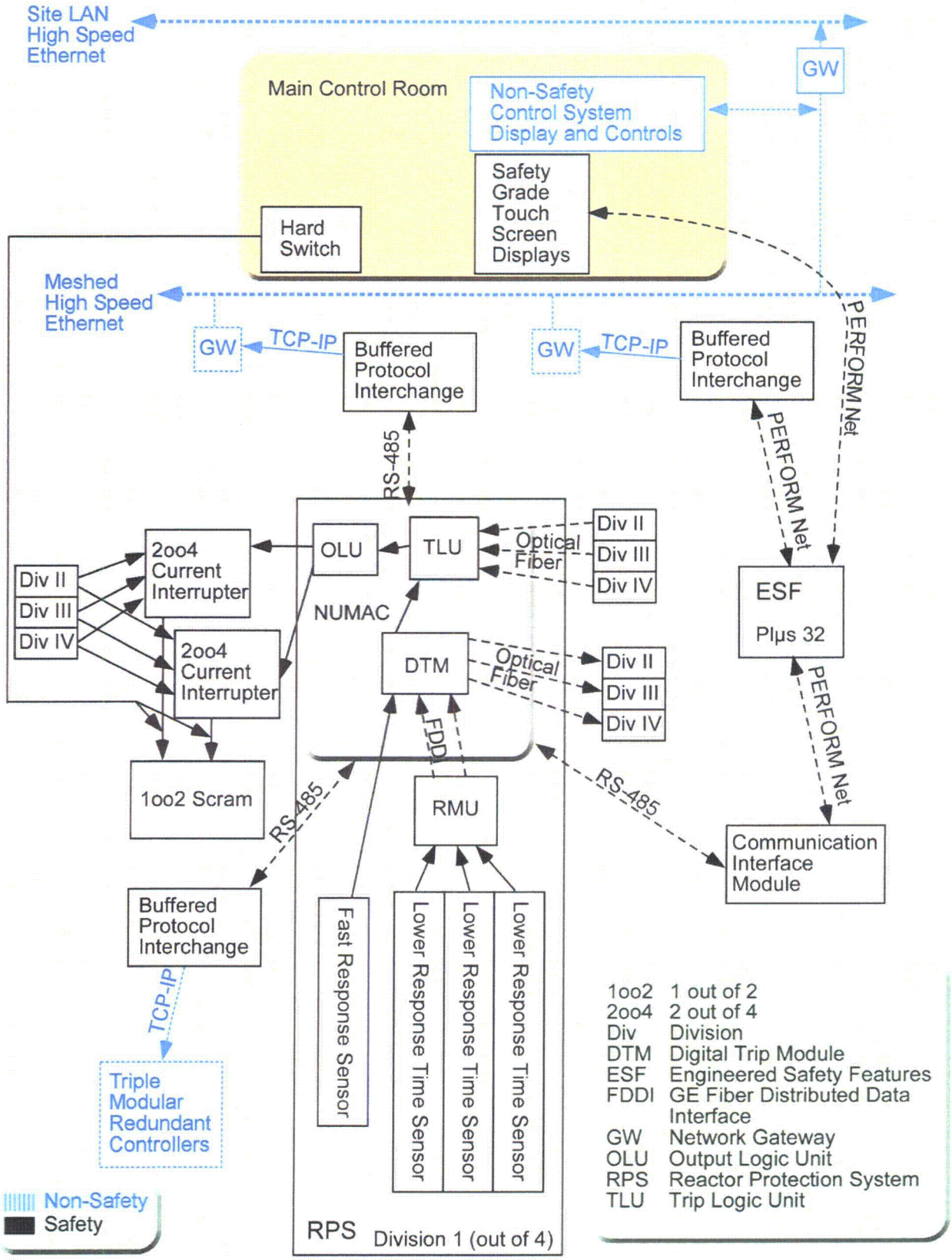

Fig. 3.5. Lungmen reactor protection system communications paths and protocols.

- 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 communication interface 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. 3.5 indicate direction of information flow. Dashed lines indicate optical fiber communication paths. Blue components are nonsafety, and black components are safety grade.

3.6.2 Engineered Safety System Architecture

The Lungmen ESF system is implemented using the Programmable Logic Microprocessor System: 32 bit (PlμS 32) from Data & Research Services (DRS). The ESF system network topology is a dual-redundant fiber optic ring with deterministic timing referred to as the essential multiplexing system (EMS). 3.6 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 in Fig. 3.6 corresponds to the ring in a division with which the unit is connected. Variegated lines indicate that the unit is connected to both rings within a division.

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 (512K bytes for Lungmen). The memory is segmented into 4K byte blocks with each block assigned to a particular node. Each node can only write to its own 4K 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

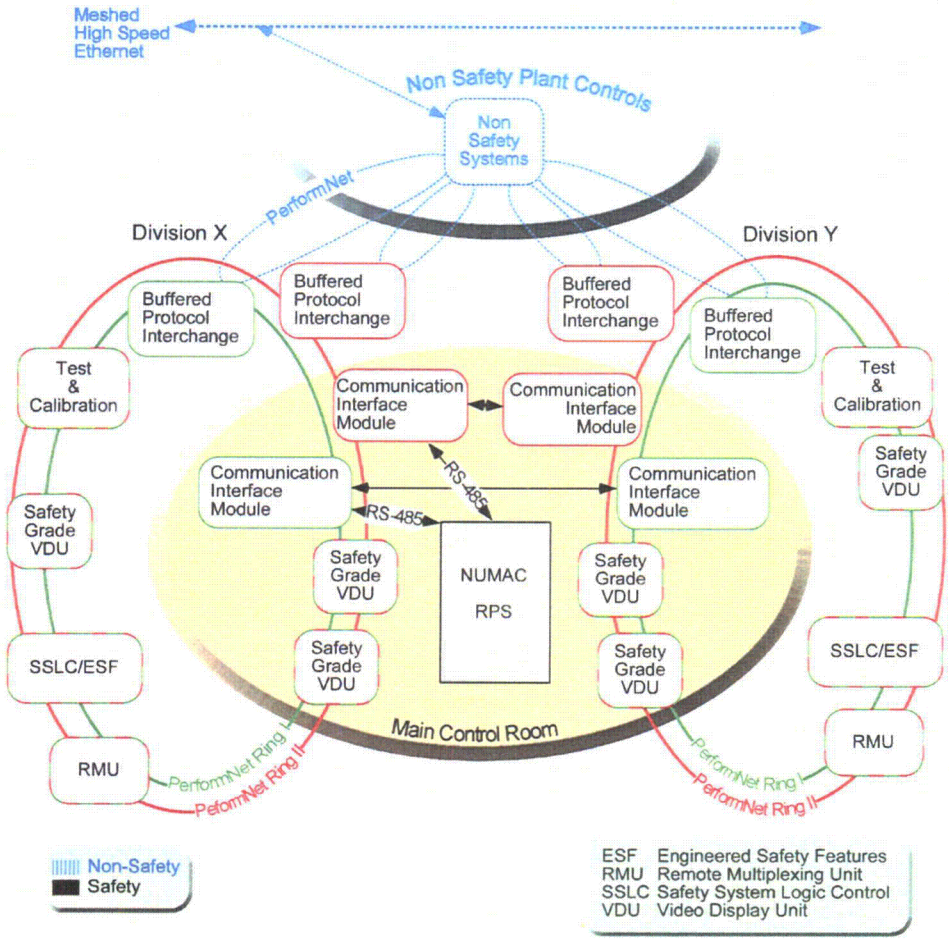

Fig. 3.6. Lungmen essential multiplexing system network topology.

separate interface modules, each accessing one of the rings of the set. Each node thus contains a complete set of the ring's 512K byte data set. Each EMS ring is connected to the nonsafety control system via a separate PERFORM network.

3.7 Temelin (Czech Republic)

The Temelin Nuclear Power Plant is a Russian-designed VVER* 1000 PWR plant. (See Refs. 29, 30.) 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

*Vodo-Vodyanoi Energetichesky Reactor.

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 engineered safety feature actuation cabinet (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. 3.7.

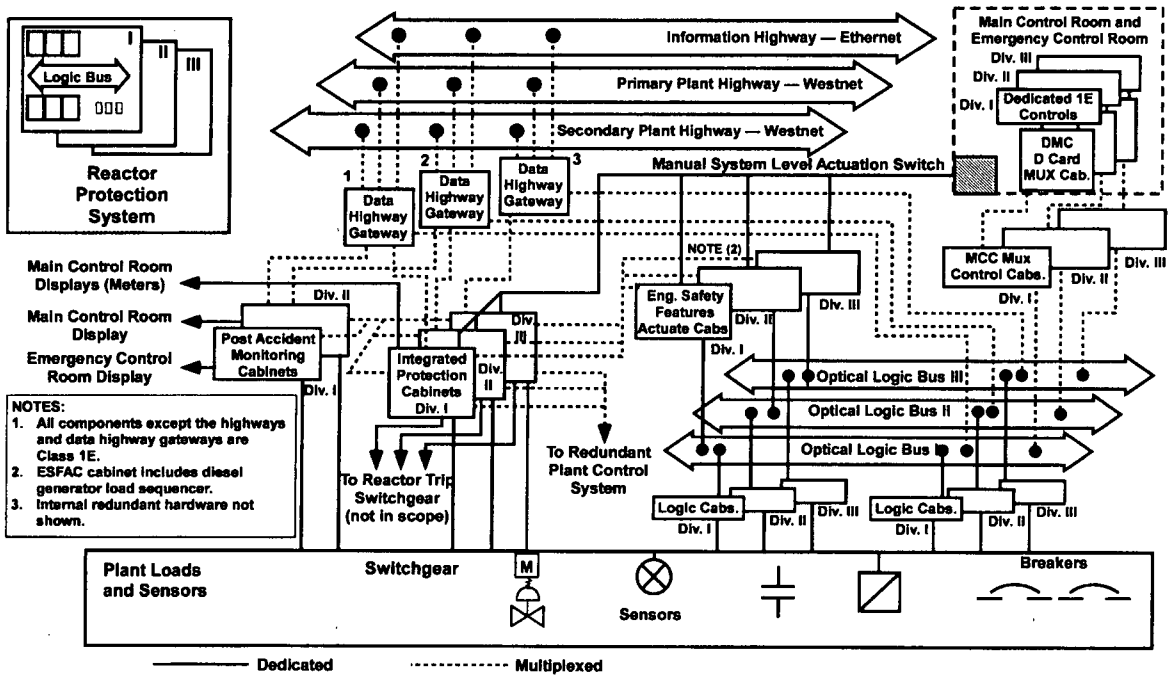

Fig. 3.7. Temelin reactor protection system. *Adapted from* W. C. Gangloff and C. L. Werner, "I&C Modernization for VVER Reactors," *IEEE Transactions on Nuclear Science* **40**(4), 819–825 (August 1993).

3.8 Dukovany (Czech Republic)

The Dukovany Nuclear Power Plant Unit 3 is a pressurized-water plant of the VVER/V213 design located in Trebic in the Czech Republic (see Ref. 31). 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.

3.9 Olkiluoto-3 (Finland)

The European Pressurized Reactor (EPR) is an advanced evolutionary pressurized water reactor (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.

3.9.1 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. 3.8. 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 (Ref. 32).

Priority Actuation and Control (PAC) modules monitor and control both safety-related and nonsafety-related actuators. Each actuator being controlled requires a separate PAC module (Fig. 3.9). 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 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. 3.9. 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, Reactor Control, Surveillance, and Limitation (RCSL), or the SAAS, or the TELEPERM XP (TXP) of the SAS.

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

Source: Personal communication with Mark Burzynski, AREVA.

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.

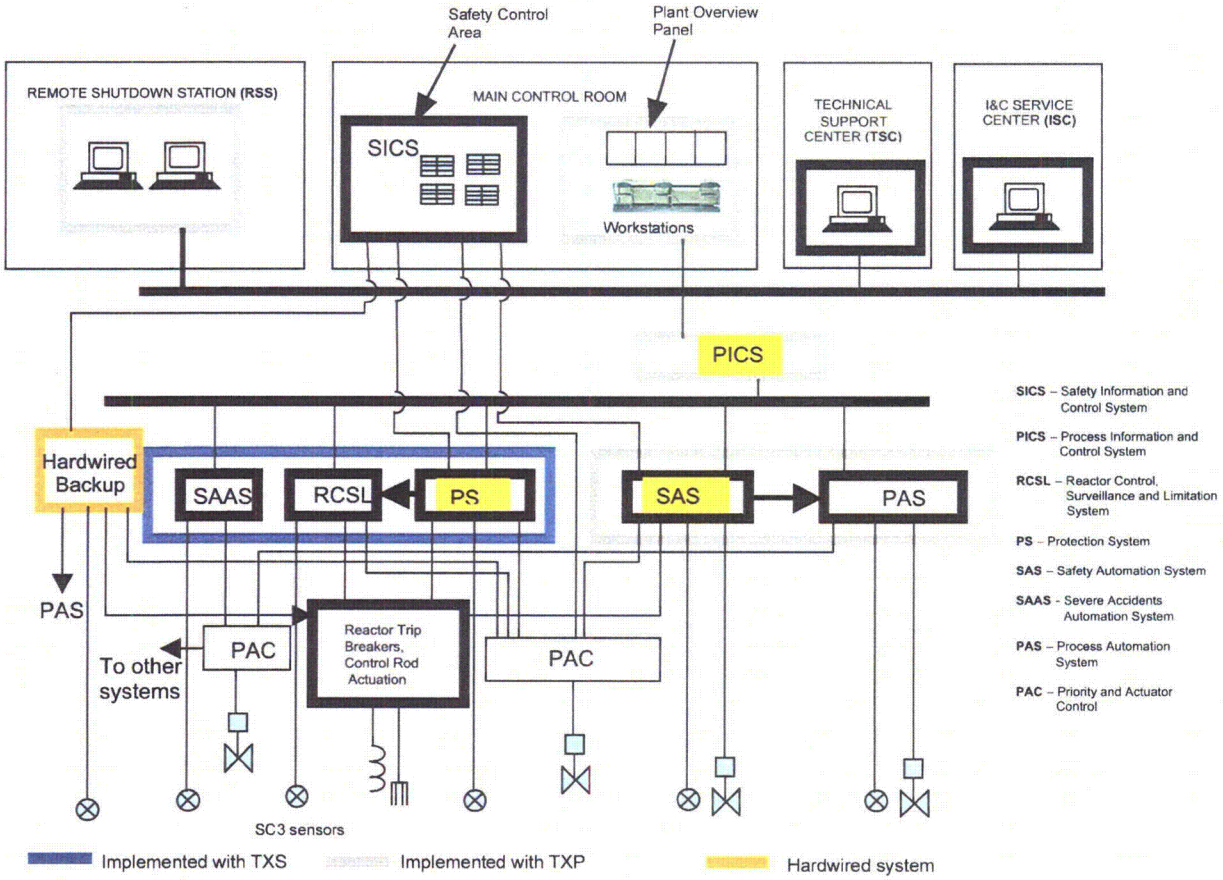

Fig. 3.8. Olkiluoto 3 I&C architecture. *Adapted from* J. Hyvarinen, STUK (see Ref. 32).

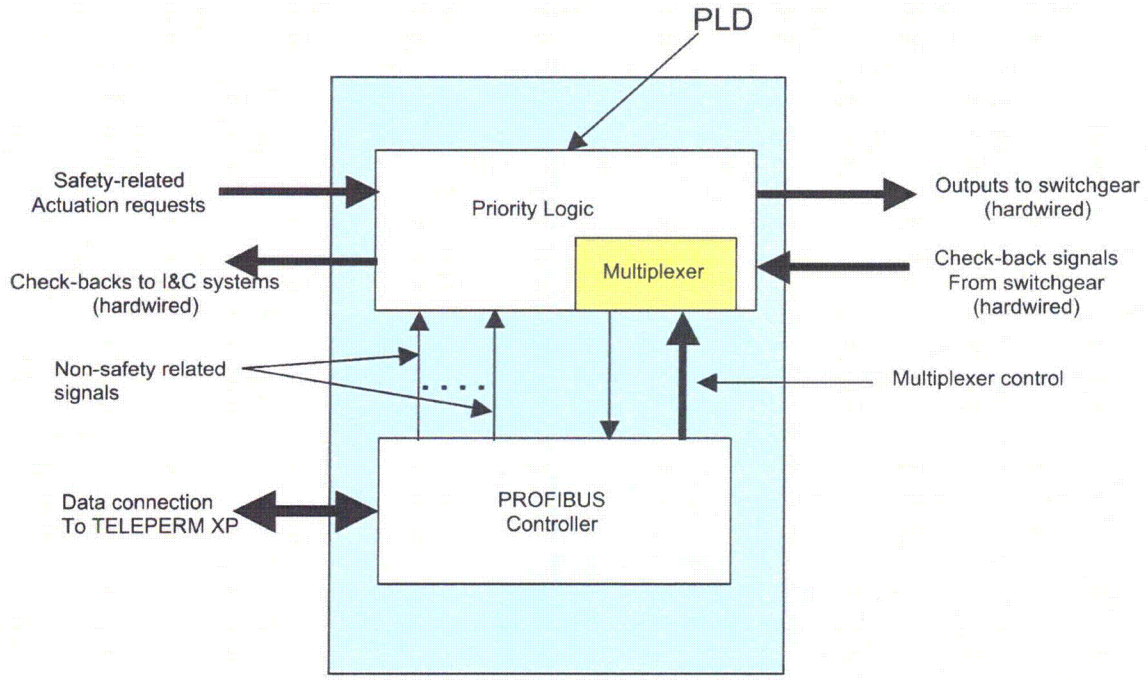

Fig. 3.9. Block diagram of Olkiluoto 3 priority and actuation module (based on Ref. 32).

At the time of writing, two different types of priority actuation modules had been proposed for the OL-3. This is in an effort to diversify the priority logic. One type is the AV42 and the other is the PC 10. There is diversity between these two types with regard to manufacturer, working principle, and the main chip set used. The AV42 was developed by Siemens AG, while the PC 10 was developed by Heitec AG. The AV42 uses Altera Max 9400LC84-20/DPC31 with 144 pins, while the PC 10 employs Altera Max EPM7256AETC100-10, with 100 pins. While both types use Altera FPGA chips and use similar tools in design development, everything else (e.g., logic design) differs.

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. The system processes data asynchronously; that is, 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.

3.9.1.1 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* (Ref. 33). Note that OL-3 uses two-way communication between PICS and PS/SAS.

3.9.1.2 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) (Ref. 33). However, partial trip data is shared between divisions for voting. Measured sensor signals are also shared for the purpose of signal validation.

3.9.1.3 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.

3.9.1.4 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 verification and validation (V&V),
- operating experience with standard library of application software function locks, and
- communication independence measures.

3.9.2 Digital I&C Issues and How They Are Addressed in the EPR

3.10 shows the Monitoring and Service Interface (MSI), not shown in Fig. 3.8, 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 computer (Fig. 3.10) 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.

*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.

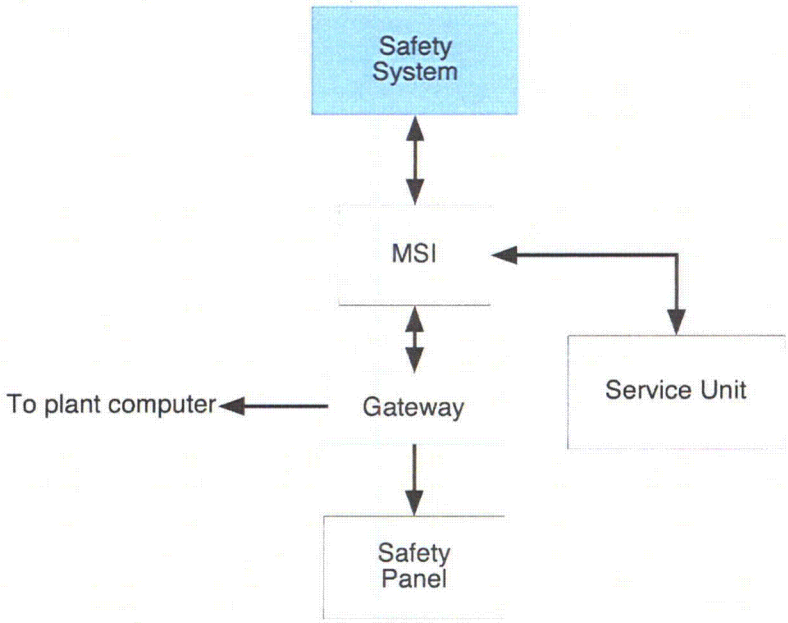

Fig. 3.10. The MSI forms a logical boundary between the rest of the safety system and the nonsafety interfaces.

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 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.

3.10 Synthesis of Technical Information from International Reactor Experience

Both U.S. and international nuclear power regulatory bodies periodically publish their regulatory principles for digital communication architectures. However, the acceptance criteria for digital

*This is also true for the U.S. EPR.
†The TXS equipment cabinets are located in the control room for Oconee.

communication topologies provides little guidance as to whether any particular implementation methodology provides reasonable assurance for achieving them. Further while probabilistic analysis as a means for achieving reasonable assurance is becoming more common in design and analysis tools, probabilistic digital system analysis has not been fully embraced by any nuclear power regulatory authority. Indeed, the international consensus standard on NPPs—*Instrumentation and control for systems important to safety—General requirements for systems* (IEC 61513)—specifically limits its scope *to exclude* additional national regulations.

A few consensus regulatory practices have emerged from investigating deployed digital I&C systems:

1. No nuclear power regulatory authority has permitted two-way communication or command of the highest class of safety system from non-safety-classified systems.
2. In all NPP regulatory schemes, communications to the highest grade of safety system are always from a high-quality, regulated system but not necessarily from the highest class of safety system.
3. For all but the simplest communications (protocol handshaking), the highest class safety system must be in bypass to accept communication access.
4. Both logical and physical access controls are universally employed for implementing changes to safety system performance (this also serves as a primary cybersecurity tool).
5. In some cases, software updates can be performed following a physical enable with the hardware installed and bypassed. In others, physical hardware replacement is required to perform software upgrades.

The lack of unambiguous guidance on evaluating the acceptability of digital communication systems means that in all cases some degree of engineering judgment has been required to approve the safety system design, architecture, and function. The specific methodology for applying this regulatory engineering judgment varies from nation to nation. To some extent, the United States is at a disadvantage as compared to other nations because its period of dormancy in NPP construction (and to a large extent even upgrades) coincided with the initial phases of the digital instrumentation revolution. Thus, the U.S. regulatory process is presented with more advanced digital system architectures with only a limited version of the two to three decades of gradual adoption of digital I&C performed in other nuclear power nations. As an example, Japanese NPPs have adopted digital technology into safety applications as part of a gradual progression from application in subsidiary, nonsafety systems, to control systems, to lower class safety systems, to top-tier safety systems. Similarly, the French progression for adopting digital technology into its safety system involved originally employing it in lower classification systems and then allowing the technology to progress into higher class safety systems as confidence was gained through experience. The United States, in contrast, has the most coarsely graduated safety categorization scheme of any nation (safety and nonsafety). The coarseness of the categorization has limited the gradual progression of digital topologies into U.S. NPP safety systems.

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. 34. Documents specifically described in the following subsections are IEEE 603-1998, IEEE 7-4.3.2-2003, IEC 61500, IEC 61508, IEC 61513, IEC 61784-3, VTT Research Notes 2265, and the European Workshop on Industrial Computer Systems (EWICS) TC7 (Ref. 35). Other useful documents not included in the review are IEC 60880-2006 (Ref. 36) and IEC 61226-2005. Standards and guidance documents reviewed or referenced in this report are listed in Appendix E with associated NRC endorsements from Regulatory Guides, NUREGs, SECY papers, and staff guidance documents.

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 should 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 IEEE 7-4.3.2-2003 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 example implementation of the buffering scheme is shown in Fig. 4.2.

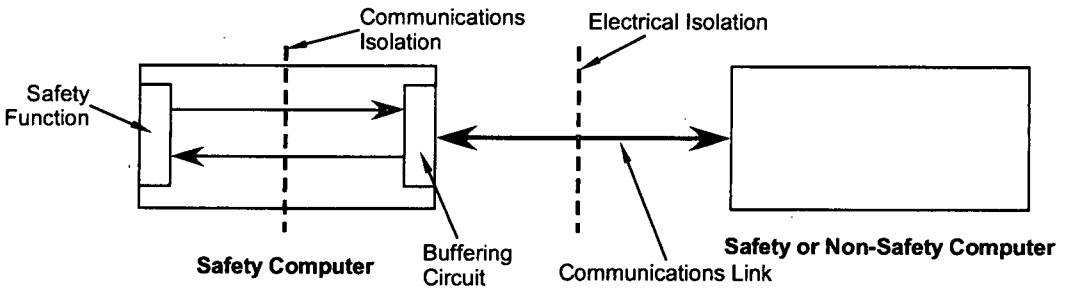

Fig. 4.1. Concept of communication buffering from IEEE 7-4.3.2-2003 Annex E.

*Note that Informational Annex of IEEE 7-4.3.2-2003 is not actually part of the standard. The annex is not endorsed by NRC.

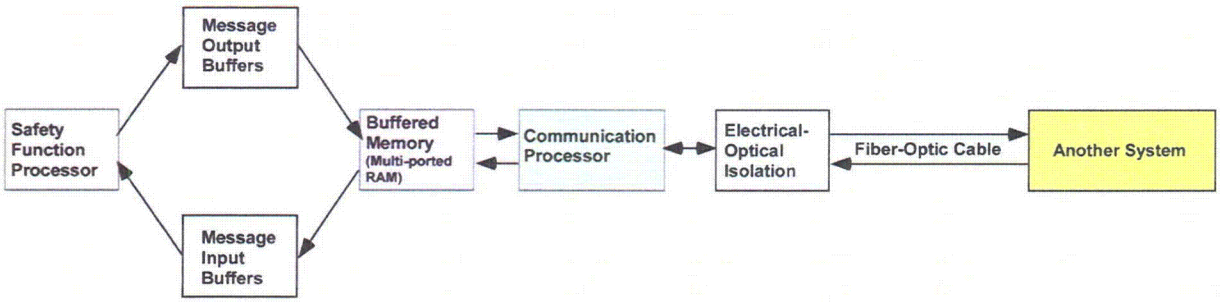

Fig. 4.2. Possible implementation of communication buffering using multiported memory.

The key feature of buffered communication is that loading and timing 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.

The regulatory position with regard to criteria for digital safety systems in nuclear power plants is embodied in Regulatory Guide (RG) 1.52, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants." The RG does not endorse Annex E of IEEE 7-4.3.2-2003 because "it provides insufficient guidance." The RG points to additional guidance as provided in Appendix 7.0-A, "Review Process for Digital Instrumentation and Control Systems," Appendix 7.1-C, "Guidance for Evaluation of Conformance to IEEE Std. 603," and Sect. 7.9, "Data Communication Systems," in NUREG-0800 (Ref. 37).

4.1.2 IEC 61500

The IEC 61500 standard (Ref. 38), "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

- electrical isolation and physical separation 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 conveyance of 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 features add complexity to the system.

4.1.3 IEC 61508 and IEC 61513

IEC 61508 (Ref. 39) 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 (Ref. 40) 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.

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 (Refs. 41, 42) address extensions to the Fieldbus technologies described in IEC 61158 (Ref. 43), 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:

FOUNDATION® Fieldbus,
ControlNet™,
PROFIBUS,
P-NET®,
WorldFIP®,
INTERBUS®, and
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.

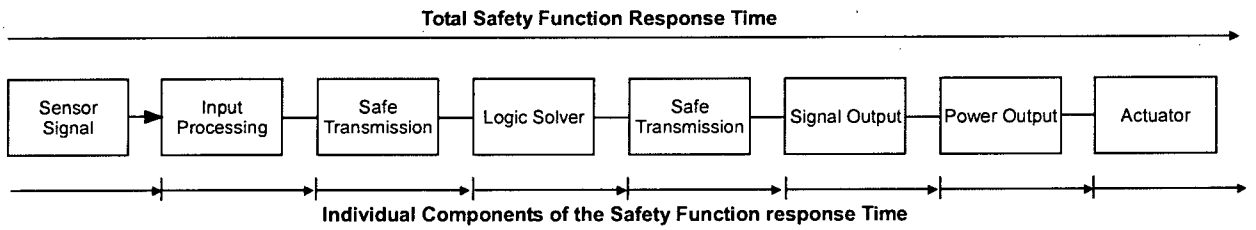

Fig. 4.3. Example of safety-function response time components.

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.

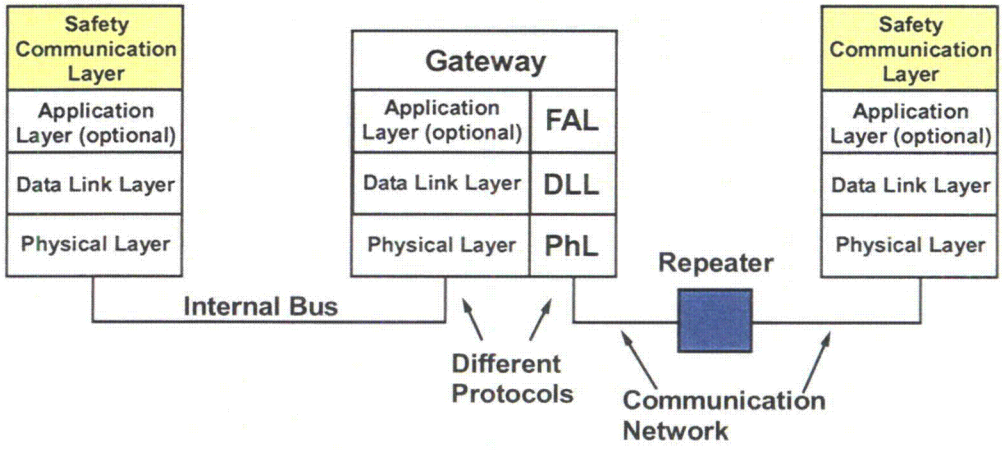

Fig. 4.4. Three-level layer model with SCL applied to a safety system network. This figure is similar to Fig. 2.3 except with the SCL added.

A safety layer, for example, 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

Section 5.4 of IEC 61784-3 lists measures commonly used to detect (and defend against) deterministic errors of communication systems. A brief description of the list is presented as follows.

Sequence number—A sequence number is appended to the body of the message as additional bits, in a predetermined way before transmission. After reception, this unique number is used to identify the actual message. Generally, these are known sequences of bits, with very good cross-correlation property under channel corruptions.

Table 4.1. Overview of measure effectiveness on possible communication errors

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[a]	
Unintended Repetition	X	X					X	
Incorrect Sequence	X	X					X	
Loss	X				X		X	
Unacceptable Delay		X	X[b]					
Insertion	X			X[c,d]	X[c]		X	
Masquerade				X[c]	X[c]			X
Addressing				X				

[a]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.

[b]Required in all cases.

[c]Depends on the application.

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

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").

Time stamp—In most cases, the content of the message is only valid for a particular time window. The time information in a message in the form of time or time and date is stamped before transmission. Relative time stamps (with respect to message sequences) or absolute time stamps can be used. Time stamping requires a reference time for synchronization. Note that "synchronization" itself is a part of the message estimation (detection and decoding), which is different from the time stamp.

Time expectation—The message sink verifies the time elapsed between two consecutive received messages against the maximum predetermined allowed delay. If this delay exceeds the maximum delay, an error is reported. For example, in time-division multiple access (TDMA) technique, each user (source) is allowed a time slot to transmit information. No one else can interfere with the designated users signal during that allotted slot. More information about timing is presented in Appendix F.

Connection authentication—Message has a unique source and/or destination identifier that describes the logical address of the safety-related participant.

Feedback message—The message sink returns a feedback message to the source to confirm reception of the original message. The feedback message has to be verified by the safety communication layers. The feedback messages can be a short acknowledgement or the acknowledgment with a copy of the original message.

Data integrity assurance—No communication system is error free, so error detection/correction is the key to reliable communications. The qualities of error detection scheme are based on trading off two antagonistic factors: minimizing the redundant information transmitted vs maximizing the error detection capability.

CRC error detection method is widely used in many communication protocols. A check sequence (typically 16 or 32-bit) is calculated by modulo-2 division of the message by a binary polynomial. The check sequence is appended as redundant bits (not the part of the actual information bits) before modulation. At the receiver, these CRC bits determine the number of bits in error. The various protocols that use CRC differ only by the polynomial chosen for the calculation. CRC does not add the bandwidth constraint of the modern error correction techniques but also does not offer powerful error correction capability. CRCs are generally used for serial communications because of their sensitivity to burst error bits, a type of error that occurs in packet-based, wireless, or interference-limited channels. Addition techniques such as interleaving can be augmented to overcome the burst error.

Error detection or correction techniques typically include redundant data in the message. These techniques are not acceptable for safety-related applications if they are not designed from the point of view of functional safety because of the potential for loss of data timeliness. Communication systems used for safety-related applications may use methods such as cryptography to ensure data integrity instead of CRC-type error detection techniques or a combination of error correction coding (convolutional type coding) and the cryptography.

Redundancy with cross checking—In safety-related applications, the safety data may be sent twice, within one or two separate messages, using identical or different integrity measures. At the sink, the transmitted safety data are cross-checked for validity. An error is determined if a difference is detected. A variety of fault detection models for safety device connections and protocols can be employed. The following are four different redundancy examples: (a) One channel is connected to the bus. Data from both safety communication layers are safety checked and cross-checked. If cross-checking shows any discrepancy, an appropriate action is initiated to maintain safety. (b) All safety communication layers, transmission layers, and transmission media exist twice. Note that transmission layers and transmission media can be of different types. (c) Everything is the same as in (b) except one transmission medium. (d) Similar to model in (a) except both safety communication layers can access the transmission layers independently.

Different data integrity assurance systems—If safety-relevant (SR) and nonsafety-relevant (NSR) data are transmitted using the same transmission medium, different data integrity assurance systems should be used, and more importantly, better encoding should be used for SR transmission to make sure that NSR information cannot influence any safety function in an SR receiver.

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 one or more corresponding safety measures are displayed against 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, because no active nuclear plant performs a SIL 4 function, reactor safety systems are typically designed and developed as SIL 4 systems.)

---

*Safety Integrity Level (SIL) is defined as a relative level of risk reduction provided by a safety function. Four SIL levels are defined in IEC 61508 [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] and IEC 61511 (IEC 61511, *Functional safety - Safety instrumented systems for the process industry sector*, Part 1: Framework, definitions, system, hardware and software requirements December 19, 2003, Part 2: Guidelines for the application of IEC 61511-1 July 12, 2004, Part 3: Guidance for the determination of the required safety integrity levels, October 18, 2004), with SIL4 being the most dependable and SIL1 being the least. The requirements for a given SIL are not consistent among all of the functional safety standards.

4.1.4.4 Data Integrity Considerations

Data integrity assurance is a fundamental component of the safety communication layer to achieve required SIL. However, a probability of bit/symbol error (Pe) exists within a correctly received frame of message due to noise and interference in the transmission media. As a result, if a bit or bits are corrupted in a correctly received message frame, the entire frame becomes erroneous. Various error detection techniques such as CRC or error correction techniques can be employed to improve Pe. The superimposed safety communication layer needs to be independent from the transmission layer. Thus, these two layers should not employ the same error detection methodology.

Any particular SIL will have a residual error rate for the safety communication layer. Advanced signal processing techniques for the physical layer can provide very low bit/symbol error rate resulting in low residual error rate for the safety communication layer. The overall residual error rate also can be reduced by having more diversity (redundancy) of the transmission paths. The residual error rate resulting from a particular transmission medium with a selected protocol of data transmission (a fixed value of Pe) can be expressed as

$$\Lambda_{SL}(Pe) = R_{SL}(Pe) * v * m \quad , \tag{1}$$

where Pe is the bit/symbol error probability of the message, $R_{SL}(Pe)$ is the residual error probability of the safety message (sequence of bits with error detection capability), v is the maximum rate of the safety messages (e.g., per hour), and m is the maximum number of destinations served by a single safety function. For example, if $Pe = 10^{-3}$, the value of residual error rate $\Lambda_{SL}(Pe) = 10^{-7}/\text{h}$ for a selected error detection/correction capability. If the system requires high demand for the safety message rate, the required value of $\Lambda_{SL}(Pe)$ is even lower in order to maintain same SIL.

4.1.4.5 Black Channels

A potentially useful 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 (Ref. 44). Its use as 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).

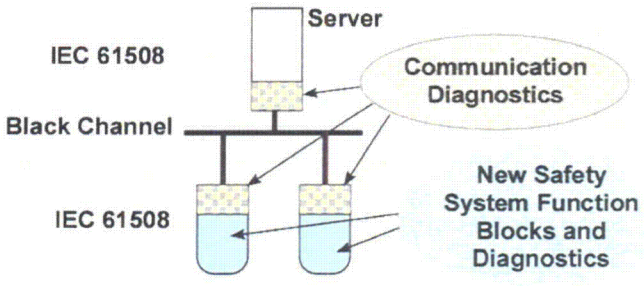

Fig. 4.5. Illustration of black channel implementation.

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.

4.1.4.6 Security Perspective

The standard includes the observation that

> "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 those that 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 (Ref. 45).

Cybersecurity as it relates to communications between safety and nonsafety systems is an important issue. The next section deals at a basic level with cybersecurity issues related to safety-to-nonsafety and interdivisional communications. Nevertheless, the authors recommend launching an investigation into related current work and standards including IEC 61784-4 (Ref. 46), which has just started development.

4.1.5 VTT Research Notes 2265

This VTT report deals with safety-related serial communications in machine automation for numerous industrial applications. (See Ref. 47.) The message error types relating to serial-mode data transmission and their remedies are thoroughly described in the report. The report derives many of its recommendations from other safety-related communication standards such as the IEC 61874-3 standard.

Although most of the safety bus solutions are commercially available, additional safety bus solutions derived from standards are also suggested in the report. Each bus solution has its own merits and poses specific challenges for safety application. For using a bus for safety application, a thorough safety analysis and testing effort is required. The report suggests that industrial users tend to integrate safety and nonsafety buses to improve the overall performance; however, the safety bus and the normal communication bus should be separated for the following reasons: If the system changes from time-to-time for application purposes, the validation of the integrated system becomes quite cumbersome and risky. Individual sanity checks and "what if" analyses are much tractable for separated systems; that is, the normal bus and the safety bus are isolated. Secondly, any new addition or system modification changes the overall safety requirement, which should be reevaluated as if it is a new system.

A generic safety analysis tool (at signal level) for bus-based communication systems is presented in the VTT report. The tool consists of a test flowchart, a database consisting of possible causes of safety failure, and various action items arranged in stages. This tool is a general procedural methodology that

can be adapted for analysis of safety buses in NPPs. Some relevant details about VTT Research Notes 2265 are presented in Appendix G.

4.1.6 European Workshop on Industrial Computer Systems (EWICS) TC7: Safety, Reliability, and Security

These guidelines concentrate on safety-critical distributed systems that may have catastrophic consequences upon failure. This EWICS report (Ref. 48) provides guidance on achieving safety in industrial computer-based distributed systems over the system's life-cycle. The EWICS report focuses exclusively on those aspects of distributed computer systems that influence the safety of the system.

System distribution may result from different design considerations such as redundancy, diversity, functional partitioning, adaptation to a geographically distributed process, or to cope with system time-response increases through local intelligence at system peripheral levels. Diversity and functional partitioning result in better safety performance according to the report. However, distributed processing and solutions to cope with longer system time-response increase the complexity of the system. This increase in complexity and underlying functionality to support distribution leads to an increase in failure modes that have to be considered within the system safety analysis. Many of these safety properties are similar to those found in nuclear power safety systems.

The EWICS report presents various aspects of basic activities of distributed systems throughout the life cycle. These are safety analysis, system requirements specification, system design, hardware design, software design, software implementation, integration, installation, operation, maintenance and modification, and replacement. Some generic aspects of distributed systems that have impact on safety are also listed. These are security, project management, verification and validation, assessment, and human factors. Safety aspects, constraints, qualities, and guidelines are listed for each of these parameters. Some sample, relevant guidance is included in Appendix H. A complete list is available in Ref. 10.

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 that have been drawn from the reviewed standards and guidance.

1. 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).
2. 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.
3. 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.
4. The system should be simple so that the probability is minimized that it contains hidden flaws due to requirements or design errors. 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 necessitate 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.

5. 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.

6. 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. The black channel concept does not appear suitable for the highest safety grade system.

7. 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 report. However, it is worth noting that security for industrial instrument networks is driven by concerns different from 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.

5. EQUIPMENT QUALIFICATION AND COMMUNICATION SECURITY

5.1 Qualification Guidance

This section provides recommendations for functional guidance with regard to communication between safety systems and systems that are nonsafety related. This Section addresses testing and aging issues related to equipment that might be used for communication between safety systems and for communication from nonsafety to safety systems. This guidance is derived from IEEE Std. 323-2003 and RG 1.209. IEEE Std. 323-2003 defines qualification as "the generation and maintenance of evidence to ensure that equipment will operate on demand...." Thus, while these recommendations have been guided by current standards and regulatory guides such as IEEE Std. 323-2003 and RG 1.209, as well as the consensus research discussed in this report, they are not geared towards attempting to establish a qualified life. Rather, the recommendations are geared towards providing added assurance that the digital I&C system will operate on demand.

This section also addresses issues concerning the display of information from sources in more than one safety division as well as maintenance and test equipment used to access plant equipment in more than one safety division. It does not address issues that may exist with regard to communication between subsystems that are entirely within a single safety division.

An attempt has been made to ensure that the recommendations provided in this section do not contradict existing regulatory guidance or requirements. Existing guidance and documentation on defense-in-depth, common cause failure protection, single failure criterion, environmental qualification, and self-checking and testing have been taken into consideration in providing these recommendations.

1. *Total Safety System Testing*—Qualification testing involving redundant safety systems should be performed on the total system as a whole and should be performed while the system is in operation (dynamic system testing). Digital (communication) systems should be qualified for the anticipated normal, accident, and postaccident environments and with due consideration to any potential degradation in their normal operating environment. For example, while optical fibers are immune to EMRI/RFI in their operating environment, some fibers may be susceptible to gradual degradation over long-term exposure to radiation or other environmental conditions such as heat.

2. *Nonsafety System Communication*—A nonsafety system involved in (networked) communication with safety systems while the safety systems are active can only be either (a) reading from the safety system(s) or (b) writing to another nonsafety system. Nonetheless the nonsafety systems and their data links to the safety system(s) should be treated as *associated circuits* to the safety system. Thus, (dynamic) qualification testing should include the nonsafety systems to ensure that the total system will operate as intended.

3. *I&C Systems Testing*—Qualification testing of the safety systems should be performed with the I&C system functioning (Ref. 49). This should include software and diagnostics that are representative of those used in actual operation, while the system is subjected to the specified environmental service conditions, including abnormal operational occurrences. Testing should exercise all portions of the safety-related computer-based I&C systems necessary to accomplish the safety-related function or those portions whose operation or failure could impair the safety-related function.

4. *Digital Worst Case Testing*—An objective of qualification testing should be to verify that the response all_digital interfaces or subsystems under worst-case conditions will still allow the system as a whole to perform its safety function within the specified time and to verify that the design accommodates the potential impact of environmental effects on the overall response of the system.

This is especially important in situations where testing the system as one unit may not be practical. Testing the safety system(s) as one unit is the preferred method if this is practicable. This is especially true of electromagnetic interference/radio-frequency interference (EMI/RFI)-prone areas, in which common cause failure due to EMI/RFI may be a significant issue.

5. *EMI/RFI Testing*—Functional and operational issues related to safety in the NPP environment should address the possibility of upsets and malfunctions in I&C systems caused by EMI/RFI and power surges. Regulatory Guide 1.180 (Ref. 50) provides adequate guidance for the design, installation, and testing practices for addressing the effects of EMI/RFI and power surges on safety-related I&C systems. This regulatory guide endorses both domestic and international EMI/RFI susceptibility standards such as Military Standard MIL-STD-461E (Ref. 51) and the IEC 61000 (Ref. 52) series of EMI/RFI test methods.

6. *Type Testing*—Type testing (with the I&C system functioning) is the preferred method of qualification. Workstations should be qualified for the anticipated normal, accident, and postaccident environments and with due consideration to any potential degradation in their normal operating environment. If communication is by means of optical fiber cables, the statements in Recommendation 1 with regard to potential degradation of some optical fibers also apply.

7. *Nonsafety Station Environmental*—The recommendations for interdivisional communications should also apply to nonsafety stations receiving information from safety divisions. In addition, the nonsafety stations should be qualified to withstand all environmental conditions of seismic, EMI/RFI, and other applicable design basis conditions. However, since the nonsafety stations are not Class 1E, they need not demonstrate complete functionality during and after the application of the design basis event. Nonetheless, it should be shown that the nonsafety station does not produce any spurious actuation or produce any adverse effect on the system.

8. *Operator Interfaces*—Guidance on digital system's interfaces and touch screens can be addressed by present-day qualification standards such as IEEE Std. 323, which requires a licensee to identify any significant aging mechanisms for the component to be qualified. For cases in which significant aging mechanisms exist, a qualified life needs to be established. The current state of the art for assessing thermal aging is to use the Arrhenius model, which establishes aging degradation as a function of temperature and allows an estimation of thermal life at a given temperature. This model, however, may not be directly applicable to human-system interface devices. Other aging predictors may be applied such as those from the military handbook on electronics equipment reliability (Ref. 53). Other considerations in the qualification of digital systems and operator interfaces include the following:
   - — methods of accommodating aging effects in qualification such as divergence of visible touch targets and corresponding sensitive screen areas
   - — effects of age and environment on optical cables and other optical components
   - — component and system-level vulnerabilities from other stressors such as environment and operator actions

5.2 Cybersecurity Issues

Early designs for information exchange between divisions in NPP safety systems used a separate wire for each data link. Data interchange was restricted to a binary representation of trip condition. The binary trip status was implemented using analog signal levels, typically a 4- to 20-mA current or 0- to 5-V representation with the low level representing one state and high level representing the other.

This type of implementation is significantly more secure than modern digital networks because each circuit only connects two systems, is electrically isolated, and communicates a simple continuous analog

value. The nuclear power industry, however, is being driven by technology progression to the replacement of obsolete point-to-point analog communication topologies to more capable digital networks.

The sophistication of multiplexed digital communications introduces new opportunities and challenges. Multiple information sources and destinations can be realized and share a single communications medium. The medium itself is no longer limited to point-to-point communications but rather can implement a network of many nodes that can selectively communicate with each other. The structure of information content on the network can be complex and multidimensional. The network also can potentially become a powerful high-speed conduit of computer security threats including viruses, malware, and unauthorized user access. The network used in the implementation of interdivisional communications should not adversely influence the safety system function.

A safety system that utilizes networking technology for interdivisional communications should address cybersecurity issues to the same level as any other network components of the safety system (Ref. 54). The design, implementation, and operation support of the interdivisional communications network should be accomplished under the prevue of the overall cybersecurity plan for the installation. This network should be a specific part of this plan. The cybersecurity plan should be compliant with NRC directives as outlined in SECY-08-0099 (Ref 55). Guidance to applicants is included in DI&C-ISG-01 (Cyber Security) (Ref. 56).

Both external and insider attacks should be considered. The best approach to protect systems that perform top-level safety functions from cyberattacks is to isolate them. The design and implementation should avoid any kind of remote configuration. If unavoidable, use encryption technologies to secure this information transfer. A cryptographic module is recommended that complies with Federal Information Processing Standards (FIPS) 140-2 (Level 2) and uses two-factor authentication (preferably with hard tokens). Encryption products can be selected that adhere to this standard. Storage and management of encryption keys should be handled as if they are classified information because FIP 140-2 is approved for DOD information up to the SECRET level.

If communication is inevitable to external systems, especially nonsafety-related systems; communication implementation from within the safety system should be done such that the communication is controlled by the safety system (Ref. 57). Ideally, the safety system should use unidirectional communication only, for example, information dissemination instead of information being gathered from nonsafety systems (Ref. 58).

Network, or shared bus, technology that is used for interdivisional communications should only support two possible types of communications: (1) the interdivisional communications of the safety system and (2) communications to external nonsafety system elements in some extreme and exceptional cases. The following discussion addresses recommendations for both types of communications.

5.2.1 Interdivisional Network Communications

Division-to-division communications (i.e., Class 1E communications between divisions) should minimize the use of active switching components. Implementation should be with point-to-point direct cabling as much as possible. The current NRC Interim Staff Guidance specifies that point-to-point connections between divisions is the acceptable architecture for "vital" communication (e.g., trip results). If active components are used, such as packet switches or shared bus devices, they should be restricted to communications between a single pair of divisions (i.e., a private network implementation). This will eliminate any opportunity for cyberthreats from propagating from a compromised division into another division. This approach is also consistent with the single-failure criterion (Ref. 59).

Conventional IT security testing should not be performed on any communications structures used for 1E interdivisional communications while the communications structures are performing their safety

functions (Ref. 60). Any testing must be consistent and a component of the approved cybersecurity plan for the system and facility.

Remote administration access to any network or shared bus device used for 1E interdivisional communications should normally not be allowed.

5.2.2 External/Remote Nonsafety Network Communications

Any type of remote connectivity into the communication infrastructure that is used for interdivisional communications is strongly discouraged. However, it is prudent to understand that certain circumstances may dictate the need for remote connectivity justifying such a violation. Requests for remote connectivity should be rigorously examined for the necessity of such a connection. In-depth justification for such a connection should be made and the vulnerabilities posed by such connections should be documented in the cybersecurity plan. To mitigate potential paths of compromise due to a remote connection, several factors need to be considered. These include the sensitivity of the information being passed through the remote connection, the security of the remote connection point, the security of the intervening medium, the strength and types of authentication and encryption required, documentation and logging requirements, susceptibility to harm that may be caused by the connection, the trust level of individuals who have access to the remote connection, and the threat exposure at the remote connection by an adversary.

Any system or component in a digitally implemented safety system division is considered to be critical. For the purposes of definitions, any component of interdivisional communication paths that allows communications between divisions is likewise considered to be critical.

1. It is recommended that any implementation of a remote connection to a component used for interdivisional communications employ a cryptographic module that complies with Federal Information Processing Standards (FIPS) 140-2 (Level 2), and use two-factor authentication (preferably with hard tokens).
2. There should be logs automatically recorded of all remote connections.
3. Each remote system should utilize host-based firewall software that cannot be disabled by the end user, and host-based virus detection software should be utilized on the remote systems with up-to-date virus signature files.
4. All network traffic associated with the remote system should be monitored for malicious activity.
5. No public Internet exposure should be allowed on directly or indirectly connected systems.
6. Operation and user access of the remote system should be procedurally controlled under an approved cybersecurity plan.
7. For maintenance operations and testing, a laptop or mobile computer may be employed with the remote connection to the 1E interdivisional communications. Any remote connection to a component used for 1E interdivisional communications involving a laptop should include additional procedures beyond those discussed above. The laptop should be a dedicated, standalone unit that is not used for any purpose other than the support utility and functions related to the connection to the 1E interdivisional communications. It should be kept physically secure when not in use. All user access should be strictly controlled and documented. Particular attention should be given management and control of the hardware and software configuration of the laptop including the denial of alternate boot methods by securing removable media drives and communications ports (USB, Firewire, Ethernet, etc.).
8. Modifications to any files or configurations of any interdivisional communications components from a remote connection should be done in accordance with established configuration control processes.

6. STRUCTURED METHODOLOGY FOR EVALUATION OF COMMUNICATIONS

Digital communication technology facilitates data and function agglomeration to a degree that was not possible for traditional analog-based control rooms. Communication interconnections among safety system redundancies and between safety and nonsafety systems or components are more likely for highly integrated control rooms at new or upgraded NPPs. Because of the potential for communication interconnections to compromise the independence of safety functions, to provide a propagation path for errors among systems, and to introduce new failure modes for safety-related I&C systems and components, the review of interdivisional and nonsafety-to-safety communications requires a comprehensive assessment of the nature of the communication, the implementation approach, as well as the credible vulnerabilities to communication errors and corresponding mitigation approaches. The assessment of error and failure types as discussed in Sect. 2, along with review of international reactors in Sect. 3 and review of consensus practices in Sect. 4, has led to the approach described in this section. This is depicted in Fig. 6.1. The communication vulnerabilities discussed in Sect. 2, the synthesis of technical information from international reactor experience with some focus on communication (Sect. 3), and the summary of standards that address communication issues for safety systems (Sect. 4) were used as basis for the suggested communication methodology suggested in Sect. 6. The approach suggested is not meant to replace current guidance such as that provided by the Standard Review Plan (SRP), nor do

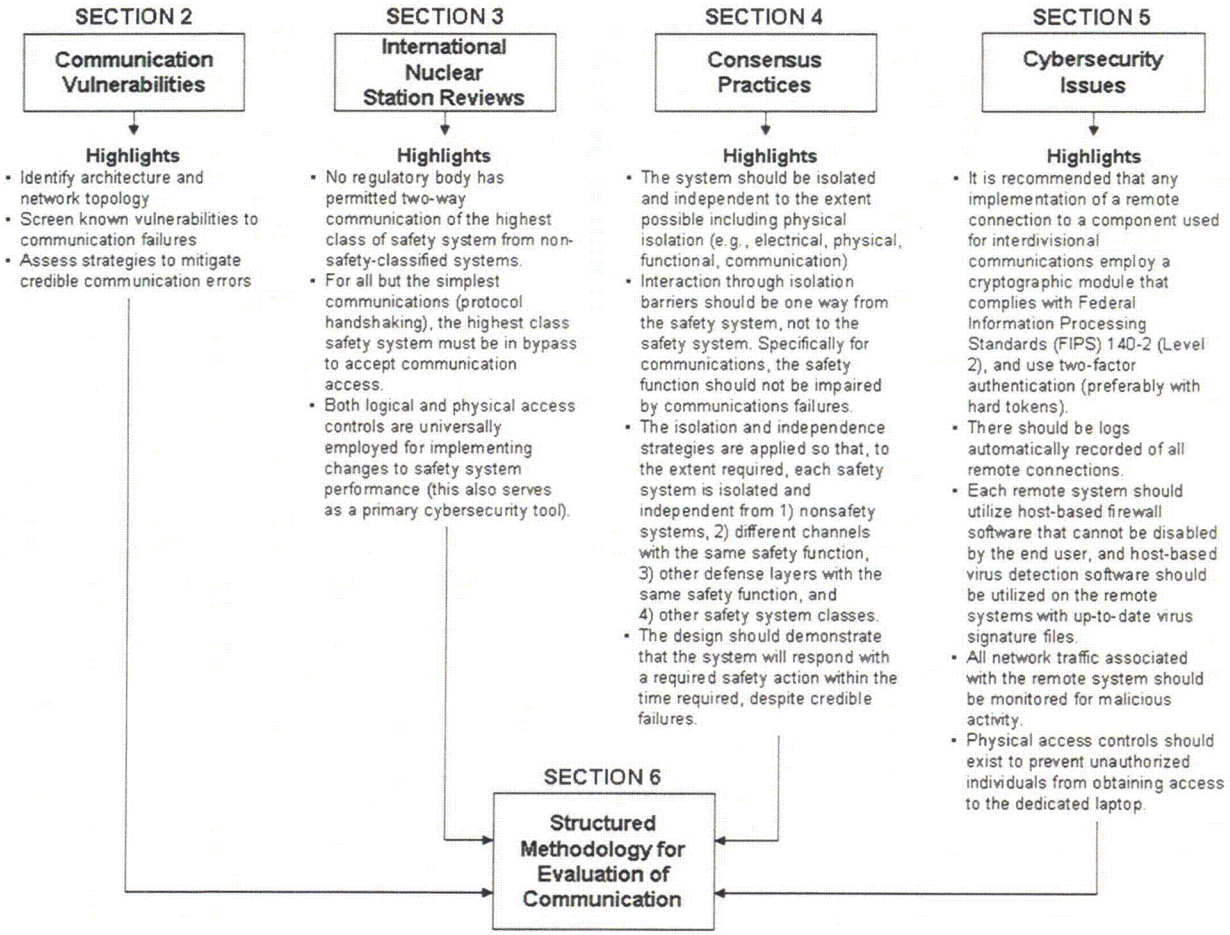

Fig. 6.1. Relationship of the information in Sects. 2, 3, 4, and 5 to the approach in Sect. 6.

they contradict this or other guidance such as those found in the Interim Staff guidance. Rather, these recommendations are intended to enhance existing guidance.

A systematic approach to assessing the acceptability of digital communication systems, either for interdivisional or nonsafety-to-safety interactions and data exchange, is to evaluate the effect of the communications on the safety function(s) and determine the capability of the architecture to avoid or withstand the occurrence of credible faults. The first element of the review approach addresses independence or, more specifically, functional dependence. The second element of the review approach addresses isolation or, effectively, execution dependence. The effect of this approach is to establish the significance of the communication and confirm that information (i.e., data or commands/requests) and interaction (i.e., communication transmission and reception) failures are accommodated in the management and processing of messages and their content.

6.2 illustrates the relationship of the dependencies and failure categories. The triggering of the dependencies by these failures results in consequences that can be characterized as (1) incorrect performance of the safety function (i.e., incorrect decision or safety response) or (2) interruption of safety function execution (i.e., code execution stops or is impeded). Information failure triggers the consequences of functional dependence, whereas transmission failure may trigger the adverse consequences of either functional or execution dependence.

The research findings in this report analyze the best practices for international reactors and how other nations address the independence, redundancy, and defense-in-depth requirements in current NRC regulations. The guidelines and acceptance criteria that follow are based on applying NRC regulations. The digital safety systems and their interdivisional and nonsafety communications do not necessitate the creation of additional regulatory positions.

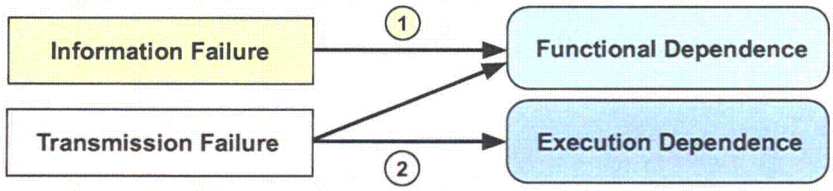

Fig. 6.2. Simple evaluation approach for safety systems communications.

6.1 Guidance for Assessment of Functional Dependence of Digital Communications

The assessment of the functional dependence introduced by communication interconnections is clearly related to confirming that the independence criterion of IEEE 603 is satisfied. The critical issue that must be evaluated is whether the communication interaction can alter, distort, or interfere with the performance of the safety function. First, the nature of the communication should be established in terms of its importance to the safety function. Next, the impact of information failures should be assessed.

The *NRC Task Working Group on Highly Integrated Control Rooms—Communications* (TWG-HICRc) has defined "vital" communication as any communication that is needed to support a safety function. Communication that enhances a safety function but is not essential to its completion could be classified as "significant" communication, while communication that neither directly supports nor enhances a safety function could be classified as "general" communication.

For interdivisional communication, vital communication, such as distributing partial trip information among safety system redundancies, provides accepted benefit to the accomplishment of the safety

function. The enhancement or benefit provided by significant communication needs to be clearly documented to enable an assessment of its acceptability. The justification for general communication must be established and evidence provided that its introduction does not add significant complexity to the implementation of the safety function for such communication to be acceptable.

For nonsafety-to-safety communication, a similar assessment can be performed to address the acceptability of establishing the communication interconnections that allow nonsafety systems to transmit messages to safety systems or components. Such communication will not be classified as vital and is not anticipated to be significant, but some communications among different safety divisions that are not vital (i.e., not for voting) could nevertheless impair the safety function if they are erroneous. Such communications should therefore be treated as significant. For example, sensor data exchange for "second-max second-min" functionality might not impede a safety function if its transmission completely failed; however, it might impede a safety function if erroneous (non-conservative) values were received instead. Thus, justification of the operational or maintenance rationale for the communication should be provided with an analysis of the consequences of failure. Such susceptibility to a single failure is justification for redundancy in transmitting those values.

After the nature and acceptability of interdivisional communication within a safety system or external communication among nonsafety and safety systems is established, the impact of information failure must be assessed to ensure that the safety function(s) is not compromised. A determination of the consequences of failure should include evaluation of the functional response to absence of information as well as an analysis of effects of undetected erroneous information. Each aspect of this review is related to confirmation that the single failure criterion has been satisfied.

In the case of information unavailability, the review relates to assessment of higher-level functional strategies. For example, if vital communication is blocked (e.g., misdirected, excessively delayed, or not transmitted), then there should be functional provisions to accommodate that condition. An obvious example is the quadruple redundancy of most digital safety system designs that provides for degraded voting schemes (i.e., 2 out of 4 $\rightarrow$ 2 out of 3 $\rightarrow$ 2 out of 2) for divisional trip decisions. While many strategies and techniques can be employed, the review should confirm that this potential susceptibility is identified and appropriately addressed in the communication system design.

In the case of erroneous information, the assessment is more complex because of the wide range of credible deviations that could be postulated for either data or commands. These information failures can be the result of uncorrected communication transaction errors, or they may be valid messages that are misdirected, out of sequence, mistimed, or miscalculated (e.g., data or parameters). Additionally, this failure category also includes incorrect interactions (e.g., inappropriate commands or requests). The scope of errors to be considered at this level of the review can be reduced by presuming that the communication protocol provides for error handling of detectable transaction errors (this capability is to be confirmed during subsequent stages of the review). What remains is to assess whether provisions are present to ensure that messages are semantically correct. An example involves use of a fixed message structure to screen corrupted or incorrect messages from further processing. Guidance on the SCL approach to high-integrity communication provides further options for treating invalid messages or incorrect data. The capability of functional mitigation strategies to handle erroneous information is not all encompassing. The transmitting system may be required to be safety grade if reasonable assurance cannot be established that the impact of credible information errors is mitigated by the SCL.

6.2 Guidance for Assessment of Execution Dependence of Digital Communications

The assessment of the execution dependence introduced by communication interconnections is related to confirming that the independence criterion of IEEE 7-4.3.2 is satisfied. The critical issue that must be evaluated is whether the communication transaction can interrupt, impede, or otherwise inhibit

the execution of the safety function. First, the implementation of the communication management should be determined. Next, the handling of transaction failures should be assessed.

Management of communication transactions requires execution of code to interface with the communication application layer. Depending on the nature of the communication interactions, interrupts associated with communication requests may exist. Additionally, higher order error-handling routines may be needed to account for certain error conditions. All of these potential conditions can place a computational burden on the CPU associated with the communications. If that processor also executes a safety function(s), then the communication activity consumes operational cycle time that could be dedicated to the safety function and self-diagnostics. Most significantly, communication error conditions can result in functional delays or processing lockup. To avoid these effects, an implementation strategy that insulates the processing of the safety function(s) from communication transaction management should be present. The TWG-HICRc has adopted the buffered circuit architecture as the preferred approach to segregate the execution of the safety function from communications activity. The buffered circuit is described in the informative Annex E of IEEE 7-4.3.2 and more fully developed normative guidance is being developed for the next revision of the standard. Essentially, a communication processor serves as a buffer between the digital network and safety function processor to ensure that normal execution of the safety function is not impeded by attention to external communication duties. The review of execution dependence should ensure that this approach or some equivalent strategy is employed to provide communication isolation. Obviously, physical separation and electrical independence are also necessary factors in addressing execution independence.

The next stage of review regarding execution dependence addresses assessment of the communication architecture, including determination of credible errors. First, it is necessary to confirm that the performance and reliability characteristics of the digital communication system are sufficient to support the communication demands. (Guidance on acceptance criteria for digital safety communications is given in the next section.) A review of the communication strategy and architecture (topology, protocol, bandwidth, etc.) should confirm that the design is adequate to satisfy the stated design requirements. Subsequently, potential vulnerabilities to communication errors should be identified and defensive measures or mitigation techniques should be established to ensure that adequate dependability (e.g., reliability, determinism, fault tolerance) is provided.

A three-step progression provides the necessary framework to perform this architectural review of digital communications. (See Sect. 2.4.) This report presents technical information describing key configuration and performance aspects of digital communication systems and identifying credible failure types associated with relevant network architectures. Using this information to guide the assessment, the following steps can enable this review process:

1. identify architecture and network topology used and note the key characteristics,
2. ensure that known vulnerabilities to communication failures and errors have been screened to define a credible set applicable to the architecture, and
3. assess the application of defensive strategies and the implementing techniques to mitigate the credible susceptibilities to communication failures and errors.

The suggested architectural review focuses on a determination of whether the digital communications design under review has systematically considered and effectively resolved the potential vulnerabilities that experience and analysis have shown to be relevant for the chosen network architecture.

6.3 Acceptance Criteria for Digital Safety Communications

All protocols used for either interdivisional or safety-to-nonsafety communication should meet the general guidance concerning characteristics of digital communication systems as follows. This applies to

both point-to-point and multidrop protocols. A discussion of issues related to protocols is given in Sect. 2. Section 5 includes qualification review guidance and acceptance criteria. The recommendations that follow are intended to provide additional detail to guidance provided in the Standard Review Plan (NUREG 0800).

6.3.1 General Networked Communications Acceptance Criteria

1. **Safety division data dependence**—The safety system divisions should be isolated and independent to the maximum 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. A safety channel should not depend on data or processing resources from another safety channel to perform its safety function, except for the purposes of voting as in the divisions of a four-channel protection system. This criterion derives from the physical, electrical, and communication independence requirements and guidelines in Regulatory Guide 1.152, IEEE Standard 603, and IEEE Standard 7-4.3.2. All channels participating in the voting should be safety channels if voting is involved in performing a safety function; that is, all the divisions should be subject to the same safety quality and qualification criteria (see Sect. 2.4; Sect. 4.2: 1-5; report DI&C-ISG-04: Sect. 1.1-1.3; Reg. Guide 1.152, IEEE Std. 603, and IEEE Std. 7-4.3.2).

   Any failure, error, and any kind of malfunction in interdivisional communication (information and signals originating outside the division) should not adversely affect the safety system function (e.g., inhibit or delay the safety function). Neither faulty communication messages nor the complete failure of a communication channel to deliver messages should inhibit the execution of the correct safety function (see also DI&C-ISG-04: Sect. 1.6, 12).

2. **Safety division failure containment**—A postulated failure in a safety channel in one division should not prevent a safety channel in another division from performing its safety function (see Sect. 4; report DI&C-ISG-04: Sect. 1.1-1.3, and IEEE Std. 603).

3. **Limitations on communication relevance**—All communication pathways to and messages received by a safety division should support or enhance the safety function performance. Justification should be provided for information received by the safety division not related to the safety function (see Sect. 4.2: 2, 3, 5 and report DI&C-ISG-04: Sect. 1.3, 1.18).

   Data communication systems should completely separate functions and information important to safety from other functions and information (see also Sect. 2 and report DI&C-ISG-04: Sect. 1.4).

4. **Nonsafety-to-safety communication**—A nonsafety system should not communicate with a safety division while the safety division is active (i.e., in operation), if that communication involves altering some portion of the information within (e.g., processor registers or memory states) the safety division. If a nonsafety system can communicate with a safety division by altering the safety system internal information (such as during testing), it should do so only when the safety division is not required to perform a safety function (e.g., when the safety system is in bypass), or when the information received by the safety division is for display purposes only (e.g., safety-related display station). If a nonsafety system can communicate with equipment within a safety division, it should do so only via a priority module, and it should be demonstrable that such communication cannot prevent the safety system of which the equipment is a part from performing its safety function. This demonstration includes an analysis for all potential modes of the nonsafety system and their impact on the safety

system (see Sect. 2; Sect. 3.10: 3; Sect. 4.2: 1–5; report DI&C-ISG-04: Sect. 1.8; and IEEE Std. 7-4.3.2).

Communication links should be designed in such a way that data communication and operation of the safety category functions cannot be jeopardized by communication with nonsafety systems. For example, tests in operation should not jeopardize the safety function (see also DI&C-ISG-04: Sect. 1.7, 9).

Data communication between safety and nonsafety systems should operate on a continuous regular cycle with a specified maximum variation in timing of transmissions. Plant and equipment conditions and failures should not cause timing inconsistency or communication saturation by message overloads under all plant conditions and for all permissible states of the network (see also DI&C-ISG-04: Sect. 1.4, 5).

Communication equipment of safety systems and nonsafety systems that are interconnected should be demonstrated to be compatible by analysis and suitable commissioning tests (see also DI&C-ISG-04: Sect. 1.13).

A single failure in a safety-grade isolator (isolating safety and nonsafety systems) must accommodate failures in the nonsafety-grade network to which it is connected unless the only credible failure of the safety-grade isolator includes disconnection from the nonsafety network (see also DI&C-ISG-04: Sects. 2.5 and 3.1).

The best approach to protect systems that perform top-level safety functions from cyberattacks is to logically isolate them. If connection is unavoidable, encryption technologies should be used to secure the information transfer. The cryptography should comply with Federal Information Processing Standards (FIPS) 140-2 (Level 2) (see Sect. 2, Sect. 3.10: 3; Sect. 4.2: 2–5; and Sect. 5.2.2: 1–6; and DI&C-ISG-01).

5. **Communications independence**—Functional independence of the safety processor should be strictly adhered to if a safety division must communicate with another safety system outside its division. Acceptable communication independence is achieved if the communication itself is performed using a dedicated communication processor, while the safety function is performed using a separate, dedicated function processor. The communications processor should only access the safety-related system through a shared dual-ported memory. The design should also ensure that the function processor's access to the shared dual-ported memory is not impeded by the communication processor. The safety function process should always have precedence in shared memory access (see Sect. 2; Sect. 3; Sect. 4.2: 1 4; report DI&C-ISG-04: Sect. 1.4; IEEE 603-1998; and IEEE 7-4.3.2-2003).

6. **Handshaking and interrupts**—To meet communication independence requirements, the safety function processor should perform no handshaking with other systems, nor should it accept interrupts from outside its own division (see Sect. 2; Sect. 3.10: 3; Sect. 4.2: 1–5; and report DI&C-ISG-04: Sect. 1.6).

7. **Message descriptions**—Messages should have predefined structure. The protocol that defines a message should have fixed locations for communication transfer control such as source and destination node, message length, and message content. Messages that do not conform to these structures should not be accepted by the receiving communication processor (see Sect. 2.4; Sect. 4.2: 4; and report DI&C-ISG-04: Sect. 1.7).

8. **Generation of inconsistent data**—Redundant safety-grade communication systems should be analyzed for potential Byzantine faults and failures and their consequences on the safety function. An example of a Byzantine fault is a digital signal that is stuck at "1/2," or in an indeterminate state. This is a voltage that is stuck anywhere between the voltage for a valid logical "0" and logical "1." Another example is a metastable flip-flop, in which the flip-flop rapidly oscillates between "0" and "1," effectively communicating different values to different observers (see Sect. 2 and discussion of Byzantine Generals' Failure provided in Appendix I).

9. **Deterministic/timely communications**—Communication among safety systems should be performed deterministically: (1) the data set to be sent and protocol used should be predetermined, and each message should be received within a predetermined time interval; (2) every message should have the same structure and sequence (e.g., message identification, status information, number of data bits) in the same relative locations in each message; (3) the message sent within each transmit cycle should include each datum, whether or not it has changed since the last transmission (see Sect. 2; Sect. 4.2: 5; report DI&C-ISG-04: Sect. 1.4, 1.7, 1.15).

   Errors or acceptable variation in communications timing should not cause a disruption to execution of the safety function (see also report DI&C-ISG-04: Sect. 1.8).

   The flow of information from each external source to a multiplexed system should be controlled by a protocol that ensures a fixed sequence of messages (see also report DI&C-ISG-04: Sect. 1.9).

   Time delays inherent in multiplexed networks should be considered systematically during design and documented to ensure that information flow, functions, and timing performance is acceptable for the most rapid required safety function response (see also report DI&C-ISG-04: Sect. 1.5).

10. **Communication redundancy**—All safety information communication between divisions except for voting should be redundantly performed with adequate speed and timing precision to ensure that the most rapidly required safety function will be reliably performed. The intent of this criterion is to address the single-failure criterion with respect to communication between safety systems (see Sect. 2; Sect. 3; Sect. 4; report DI&C-ISG-04: Sect. 1.8; and IEEE Std. 603-1991).

11. **Communication integrity**—At least one corresponding safety measure or combination of safety measures should be incorporated to defend against the defined possible communication errors (see Sect. 2.3.1; and report DI&C-ISG-04: Sect. 1.12).

    Communication with safety divisions should provide a means of ensuring that data packets to and from external sources are received correctly and in a timely manner. Data integrity should be confirmed by the receiving node of the safety-related application. An example of methods to confirm integrity are redundant data and redundancy checks like parity bits, frame checking sequence, cyclic redundancy check (CRC), and similar message redundancy forms. The communications processor (associated with a safety function processor) should detect and block commands that are found to be in error (see also report DI&C-ISG-04: Sect. 1.13).

    The communication system should provide sufficient capacity and time response to ensure that any message sent from any communications workstation on the network is received by the intended destination and that all functions important to safety are performed in all conditions envisaged in the station design basis (see also report DI&C-ISG-04: Sect. 1.16).

The communication technology should be selected and sized to meet the performance requirements under all data loads generated by anticipated plant transients (including avalanches of changes of state in case of general loss of power supplies) (see also report DI&C-ISG-04: Sect. 1.19).

A threshold based on a measurable characteristic, such as time, retries, cycles, number of corrections or errors, should be placed on all forms of error checking and data correction to force a decision regarding the status of a system's network connection. The reaching of a threshold should cause the system (a network node) to transition to a predetermined safe state or default message/data content that is established based on the safety function involved (see also report DI&C-ISG-04: Sect. 1.20).

A metric should be provided that indicates the communication design's reliability suitability. An example of such a metric is residual error rate on the safety communications system. This metric may be combined with systematic analysis to determine the suitability of the communication design for its associated safety system.

All communications interfaces and associated software should be verified for an adequate level of (1) failure detection, (2) protection against corruption, and (3) data validation.

It is desirable to provide diagnostic information and failure warnings to plant operators and maintenance personnel. However, neither real-time diagnostics nor periodic testing of communication systems should cause transmission delays or induce faults in messages sent to safety-related systems.

6.3.2 Multidivisional Control and Display Stations

Safety-related stations that receive information from other divisions that are either safety or nonsafety related:

(a) With regard to functional requirements for safety stations receiving information from either safety or nonsafety systems, recommendations 1 through 11 in the previous section (Interdivisional Communications) also apply.

Safety-related stations controlling or monitoring the operation of equipment in safety-related divisions:

(b) **Multidivisional workstation**—Safety-related workstations controlling safety equipment within other divisions should do so only by way of a priority module while the equipment is performing its safety function. The priority module should also undergo the same qualification as any other safety system (see also report DI&C-ISG-04: Sect. 2.1–2.10).

(c) **Nonsafety control blocking (inside division)**—To meet the requirement of Sect. 5.2, "Completion of Protective Action," of IEEE Standard 603, a nonsafety maintenance and testing station should not be able to influence safety equipment in its own division while the equipment is performing its safety function.

(d) **Nonsafety control blocking (outside division)**—To meet the requirement of Sect. 5.2, "Completion of Protective Action," of IEEE Standard 603, as well as independence requirements in IEEE Standard 603, a nonsafety maintenance and testing station should not be able to influence safety equipment in another division while the equipment is performing its safety function.

(e) **Bypass allowance**—A safety workstation may put a safety division in another division in bypass only when the affected safety system determines that this is acceptable (see Sect. 3.10: 3; report DI&C-ISG-04: Sect. 1.11, 3.1: 3, 4).

(f) **Reset allowance**—A safety station in one division should not be able to reset a safety command in another division unless the other safety division itself determines that the reset is acceptable. If the other safety division is not able to completely evaluate the question of whether reset is appropriate, then the reset should be performed from a safety workstation from within its own division (see Sect. 3.10: 4, 5 and report DI&C-ISG-04: Sect. 3.1: 3, 4).

(g) **Software alteration**—Safety division software should be protected from alteration while the safety division is in operation. On-line changes to safety system software should be prevented by hardwired interlocks or by physical disconnection of maintenance/monitoring equipment. A workstation (e.g., engineer/programmer station) may alter addressable constants, set points, parameters, and other settings associated with a safety function only by way of the dual-processor/shared-memory scheme described in this guidance and only when the associated channel is not performing its safety function. Such a workstation must be physically restricted from making changes in more than one division at a time. Provisions that rely on software are not acceptable (see Sect. 3.10: 5; Sect. 4.2: 7; Sect. 5.2.2: 6, 7, 8; and report DI&C-ISG-04: Sect. 1.10).

Nonsafety stations controlling or monitoring the operation of equipment in safety-related equipment:

(h) **Equipment access**—Nonsafety stations monitoring or controlling safety equipment should do so only by way of a priority module. The priority module should undergo the same qualification as any other safety system. In addition, the nonsafety datalinks and (computer) interfaces, while not Class 1E, should be developed with sound qualification practices; that is, they should undergo adequate functional and environmental qualification testing to ensure that no failure modes exist that could prevent the priority module or the safety equipment from performing its safety function (see also report DI&C-ISG-04: Sects. 2.1–20).

(i) **Nonsafety blocking**—To meet the requirement of Sect. 5.2, "Completion of Protective Action," of IEEE Standard 603, a nonsafety control station should not be able to influence safety equipment while the equipment is performing its safety function. No combination of failures from a nonsafety workstation should result in malfunction, spurious operation, or lock-up of a safety division.

(j) **Reset from nonsafety systems**—A nonsafety system should be able to place a safety system into bypass or bring a safety system out of bypass only when the safety system itself has determined that such action would be acceptable. Further, the nonsafety station may have the capability to reset a safety system condition if the safety division is already in a bypass. Nevertheless even such a case, the reset should only be allowed if the safety system itself determines that the reset action is acceptable (see also report DI&C-ISG-04: Sect. 3.1: 3).

(k) **Cyber protection**—Operation and user access of remote systems that can access interdivisional communications should be procedurally controlled under an approved cybersecurity plan. For those implementations of a remote connection to a component used for interdivisional communications in which the plan requires a cryptographic module, that module should comply with Federal Information Processing Standards (FIPS) 140 2 (Level 2), and use two-factor authentication (preferably with hard tokens). The plan should consider the benefits of automatic remote connection logging. Especially for multinode network implementations, each remote system should utilize host-based firewall software

that cannot be disabled by the end user, and host-based virus detection software should be utilized on the remote systems with up-to-date virus signature files. Network traffic associated with the remote system should be monitored for malicious activity. No public Internet exposure should be allowed on directly or indirectly connected systems. Modifications to any files or configurations of any interdivisional communications components from a remote connection should be done in accordance with established configuration control processes. For maintenance operations and testing, a laptop or mobile computer may be employed with the remote connection to the 1E interdivisional communications. Any remote connection to a component used for 1E interdivisional communications involving a laptop should include additional procedures beyond those discussed above. The laptop should be a dedicated, standalone unit that is not used for any purpose other than the support utility and functions related to the connection to the 1E interdivisional communications. It should be kept physically secure when not in use. All user access should be strictly controlled and documented. Particular attention should be given management and control of the hardware and software configuration of the laptop including the denial of alternate boot methods by securing removable media drives and communications ports (USB, Firewire, Ethernet, etc.). (see Sect. 5.2.2).

7. CONCLUSIONS

The report examines (1) failure mechanisms arising from several possible network architectures and message types, (2) international power reactor operating experience in utilizing digital network communications between safety systems, and (3) networking consensus practices adopted by various standards organizations in the United States and internationally. From these information sources, review guidance has been developed that pertains to interdivisional communications and nonsafety-to-safety communications. Further, evaluation methodology has been developed that applies the report's findings to the regulatory review process.

The international NPPs reviewed in this report have implemented digital communication more pervasively than current U.S. 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 utilize extensive digital communication that is comparable to that provided in the new U.S. 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 as the safety classification increases. Communication between systems of equivalent safety class is generally allowed. 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 buffered, one-way communication nodes in line with guidance in IEEE 7-4.3.2-2003, which recommends erecting barriers (Annex E of the standard suggests one-way buffering). DI&C-ISG-04 affirms that interdivisional communication may be bidirectional or unidirectional. Sect. 1.4 of DI&C-ISG-04 describes communications buffering at the module processor level but not at the network level. In describing credible communication faults, DI&C-ISG-04 Sect. 1.12 refers to errors introduced in buffers but does not suggest one-way communications. As noted in Sect. 3, Olkiluoto-3 (and the U.S. EPR) proposes 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 sole exception in these examples involves interface modules.

The prevailing standard for the U.S. nuclear power industry on computer-based safety systems is IEEE 7-4.3.2. The Informative Annex to the standard, which is not part of the standard itself, provides guidance on maintaining independence in systems where digital communication is employed. The annex is not endorsed by NRC. Recognizing that guidance on this topic can be enhanced to improve clarity and provide increased detail on specific approaches, the IEEE is considering a revision to the standard. As the standards committee seeks to develop an optimal standard, it 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. In some cases, these standards do provide practical recommendations for selected designs. IEC 61784-3 provides the most definitive guidance on communication systems 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.

The IEC 61784-3 standard introduces 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 is an associated concept described by IEC 61784-3 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 and does not appear to be appropriate for the highest safety class.

Equipment qualification issues are presented that relate to display of information from sources in more than one safety division. Qualification topics include qualification testing, in situ testing, and type testing. Cybersecurity issues related to communication to a safety system are briefly treated. The two major cybersecurity topics are interdivisional and external/remote (nonsafety) network communications.

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 for their use in safety systems, although the review of safety characteristics of such systems is more complex.

A structured approach for describing the vulnerabilities of safety-to-safety and nonsafety-to-safety communications systems has emerged from this study and can be summarized as follows. 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. 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). 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 a single other safety or any number of nonsafety systems should not lead to an incorrect safety decision. Where external communication is necessary, safety function dependence on communication correctness can be minimized if the implementation can accommodate erroneous, corrupted, or unanticipated information. Communication independence can be promoted by controlling the pass-through of information based on strict message formalism and validity checks.

An acceptable systematic review process for interdivisional and nonsafety-to-safety digital communication systems should address the unique issues posed by introducing interconnections among previously isolated systems, redundancies, and components. In particular, whether the communication satisfies the essential independence criteria (or results in unresolved dependences) must be evaluated. Safety system dependence on information correctness can result in interference with the performance of a safety function, while safety system dependence on communication performance can result in blocking the accomplishment of a safety function. A framework to facilitate the necessary safety review of digital communication systems for highly integrated control rooms is provided by this document and can be coupled with technical understanding of communication architectures and credible failure types. General guidance concerning characteristics of digital communication systems that are necessary to support interdivisional and nonsafety-to-safety communication is also provided.

8. REFERENCES

1. U.S. Nuclear Regulatory Commission Information Notice 93-57, "Software Problems Involving Digital Control Console Systems at Non-Power Reactors," July 23, 1993.
2. U.S. Nuclear Regulatory Commission 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.
3. IEEE Standard 796-1983, *Microcomputer Systems Bus*, approved February 17, 1984, reaffirmed January 23, 1989.
4. 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.
5. 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.
6. G. Preckshot, *Data Communications*, NUREG/CR-6082, UCRL-ID-114567, ML063530379, Lawrence Livermore National Laboratory, August 1993.
7. *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.
8. J. A. Lenner, "The Development of Safety Networks in a 61508 Environment," presented at ISA Expo 2003, www.isa.org.
9. IEC 61784-3/CDV, "Digital Data Communications for Measurement and Control," International Electrotechnical Commission, draft version 4.0.
10. I. Broster and A. Burns, "The Babbling Idiot in Event-triggered Real-time Systems," G. Fohler (ed.), pp. 25–28 in *Proceedings of the Work-In-Progress Session, 22nd IEEE Real-Time Systems Symposium*, YCS 337, Department of Computer Science, University of York, 2001.
11. C. Temple, "Avoiding the Babbling-Idiot Failure in a Time-Triggered Communication System," ftcs, p. 218, The Twenty-Eighth Annual International Symposium on Fault-Tolerant Computing, 1998.
12. H. Kopetz, *Real-Time Systems*, Kluwer Academic Publishers, 1997.
13. K. Driscoll, B. Hall, M. Paulitsch, P. Zumsteg, and H. Sivencrona, "The Real Byzantine Generals," IEEE, 2004.
14. A. Girault, C. Lavarenne, M. Sighireanu, and Y. Sorel, *Fault-Tolerant Static Scheduling for Real-Time Distributed Embedded Systems*, Institut National De Recherche En Informatique Et En Automatique, No. 4006, September 2000.
15. EN 50159-2, "Railway Applications, Communications, Signaling, and Processing Systems," Part 1: Safety-related communication in closed transmission systems, Brussels, European Committee for Electrotechnical Standardization (2001).
16. 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.
17. International Atomic Energy Agency, "Safety of Nuclear Power Plants: Design, Safety Standards," Series No. NS-R-1, IAEA, Vienna (2000).
18. 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.
19. 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.
20. International Electrotechnical Commission, IEC 61226, "Nuclear Power Plants—Instrumentation & Control Systems Important for Safety-Classification," 2005.

21. International Atomic Energy Agency, "Specification of Requirements for Upgrades Using Digital Instrument and Control Systems," IAEA-TECDOC-1066, IAEA, Vienna, 1999.
22. TELEPERM XS: A Digital Protection System, EMF-2110(NP)(A), Revision 1 Safety Evaluation Report, U.S. Nuclear Regulatory Commission, May 2000.
23. Paul Dacruz, A Practical Appreciation of the Implementation of a Fully Computerized Monitoring and Control System in N4 NPP Series: An Advanced Instrumentation and Control System," NPIC&HMIT 2006, p. 217-226.
24. Advanced Reactor Licensing: Experience with Digital I&C Technology in Evolutionary Plants, NUREG/CR-6842, ORNL/TM-2004/74, ML042360635, Oak Ridge National Laboratory, April 2004.
25. G. W. Remley, B. M. Cook, and P. A. Loftus, "Sizewell B Integrated Control and Instrumentation System: A Vision Becomes Reality," IEEE 0-7803-0883-2193.
26. 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," pp. 221–231, International Conference on 14–15 September 1992.
27. Chia-Kuang Lee, "The Network Architecture and Site Test of DCIS in Lungmen Nuclear Power Station," pp. 747–54, 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.
28. 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, Rockville, Maryland, March 13–15, 2007.
29. *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.
30. W. C. Gangloff and C. L. Werner, "I&C Modernization for VVER Reactors," *IEEE Transactions on Nuclear Science* **40**(4), 819–825 (August 1993).
31. 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.
32. J. Hyvarinen, *OL3 I&C Review Status,* ASN/IRSN-NRC-STUK Meeting, March 22, 2007.
33. *EPR Design Description*, Framatome ANP, Inc., August 2005.
34. G. Johnson, *Comparison of IEC and IEEE Standards for Computer-Based Control Systems Important to Safety*, UCRL-ID-146642, Lawrence Livermore National Laboratory, 2001.
35. Stuart Anderson and Janusz Górski, European Workshop On Industrial Computer Systems Technical Committee 7 (Safety, Reliability And Security), "Guideline On Achieving Safety In Distributed Systems," February 2002.
36. IEC 60880-2006, *Nuclear power plants. Instrumentation and control systems important to safety—Software aspects for computer-based systems performing category A functions*, May 9, 2006.
37. U.S. Nuclear Regulatory Commission, NUREG-0800, *Standard Review Plan*, Chapter 7, "Instrumentation And Controls," Revision 5, March 2007.
38. IEC 61500, "Nuclear Power Plants—Instrumentation and Control Systems Important to Safety—Data Communication," International Electrotechnical Commission, 2002.
39. 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.
40. IEC 61513, "Nuclear power plants—Instrumentation and control for systems important to safety—General requirements for systems," 2001.
41. 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.
42. IEC 61874-3, "Digital data communications for measurement and control—Part 3: Profiles for functional safety communications in industrial networks," 2006.

43. IEC 61158, *The Fieldbus standard Its influence and present status*, specification comes in six parts.
44. 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.
45. IEC 62443-3, *Network and system security*, Part 1: Terminology, concepts and models, Part 2: Establishing an industrial automation and control system security program, Part 3: Operating a manufacturing and control systems security program, Part 4: Specific security requirements for manufacturing and control systems, Part 5: Security technologies for industrial automation and control systems; no parts have issued as of September 2008.
46. IEC 61784-4, *Industrial communication networks—Profiles*, Part 1: Fieldbus profiles December 14, 2007, Part 2: Additional fieldbus profiles for real-time networks based on ISO/IEC 8802-3, Part 3-3: Functional safety fieldbuses—Additional specifications for CPF 3, Part 4: Profiles for secure communications in industrial networks, Part 5-6: Installation of fieldbuses—Installation profiles for CPF 6.
47. J. Alanen et al., "Safety of Digital Communications in Machines," VTT Research Notes 2265, October 2004.
48. European workshop on industrial computer systems technical committee 7 (EWICS TC7), "Guideline on achieving safety in distributed systems," February 2002.
49. Regulatory Guide 1.209, "Guidelines for Environmental Qualification of Safety-Related Computer-Based Instrumentation and Control Systems in Nuclear Power Plants," March 2007.
50. Regulatory Guide 1.180, "Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems," Rev. 1, October 2003.
51. Department of Defense, Military Standard MIL-STD-461E, "Requirements for the Control of Electromagnetic Interference Characteristics of Subsystems and Equipment."
52. IEC 61000, *Electromagnetic Compatibility* (EMC), nine parts first publication May 15, 1992, with numerous dates for Part issuances and maintenance.
53. Military Handbook on "Reliability Prediction of Electronic Equipment," MIL-HDBK-217F, December 1991.
54. IEEE Standard 7-4.3.2, "Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations," December 19, 2003.
55. SECY-08-0099, Final Rulemaking –Power Reactor Security requirements (RIN 3150-AG63) from R. W. Borchardt, July 9, 2008.
56. U. S. Nuclear Regulatory Commission, Interim Staff Guidance, Digital Instrumentation and Controls, DI&C-ISG-01, Cyber Security, December 31, 2007.
57. S. Anderson and J. Gorski, European Workshop on Industrial Computer Systems (EWICS) Technical Committee 7, "Guideline on Achieving Safety in Distributed Systems," February 2002.
58. "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants," U.S. Nuclear Regulatory Commission Regulatory Guide 1.152, Rev. 2, January 2006.
59. IEEE Std. 379-2000, "Standard Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems," September 21, 2000.
60. J. Weiss, "Roles for Operations and IT in Securing Cyber Vulnerabilities in Control Systems," Electric Light and Power, October 2004.

APPENDIXES A–I

APPENDIX A

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 NPPs 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 ensure 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 ensure 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 ensure 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.

---

*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 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.

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 ensure that safety is not significantly impaired.

Criterion 25. Protection System Requirements for Reactivity Control Malfunctions

The protection system shall be designed to ensure 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 ensure an extremely high probability of accomplishing their safety function in the event of anticipated operational occurrences.

APPENDIX B

OPEN SYSTEM INTERCONNECTION 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, Internet working, 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 C
MULTIPLEXING TECHNIQUES

Time Division Multiplexing/Multiple Access

In Time Division Multiplexing/Multiple Access (TDM/TDMA), the same communication resource is shared by assigning each signal from a user a short duration of time called a time slot. All the signals from incoming users can share the same frequency band available. The unused time regions between slot assignments, called guard times, allow for some time uncertainty between signals in adjacent time slots and thus act as buffer zones to reduce interference. Time is segmented into intervals called frames. Each frame is further partitioned assignable user time slots. The frame structure repeats, so that a fixed TDMA assignment continues one or more slots that periodically appear during each frame time.

The simplest TDMA scheme, called fixed-assignment TDMA, is so named because the time slots that make up each frame are preassigned to signal sources for the long term. A fixed assignment TDMA is efficient when the source requirements are predictable, and the traffic is heavy. However, for message bursts or sporadic traffic, the fixed assignment scheme is wasteful. A dynamic time slot assignment, called time-division packet switching, can be used to improve the efficiency, where more slots are available for heavier traffic and fewer slots are assigned for sporadic traffic.

Frequency-Division Multiplexing/Multiple Access (FDM/FDMA)

In Frequency-Division Multiplexing/Multiple Access (FDM/FDMA), signals such as telephone signals, each one having a fixed information bandwidth, form a multichannel composite. In frequency modulation/frequency shift keying(FM/FSK), the composite signal is frequency modulated onto a carrier before transmitting. In FDMA, subdivisions of the total available bandwidth are assigned to different users. Each user receives a specific bandwidth allocation to access the channel. Thus, composite FDM channels are FM/FSK modulated and transmitted to the desired user within the bandwidth allocation of an FDMA plan. FDMA is simpler to implement. The FDMA channels require no synchronization; each channel is almost independent of all other channels.

FDMA is often used in microwave communication systems and high-capacity broadband communication systems. FDM is not generally used in real-time control systems except for low-speed remote units connected by inexpensive telephone equipment.

Packet Multiplexing

Packet communications decouple the idea of multiplexing from the fixed bandwidth allocation inherent in TDM and FDM approaches. Rather than dedicated fixed time-slots or frequency bands as in the TDM and FDM multiplexing techniques, packets carry data stream identification with themselves, allowing continuously variable, on-demand allocation of bandwidth to individuals as needed.

Packet multiplexing has been used for an event structure model of communication such as computer communications. A rich set of protocols is available for various data communications. Although many packet multiplexing techniques are usually considered nondeterministic and are not used in critical hard real-time systems, the current trend of packet multiplexing is very promising and can be used for real-time systems in future.

In wireless communications, multiplexing can also be accomplished through alternating polarization (horizontal/vertical or clockwise/counterclockwise) on each adjacent channel and satellite, or through a phased multi-antenna array combined with a multiple-input multiple-output communications (MIMO) scheme.

APPENDIX D
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., programmable logic controller (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.,

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

locks and keys) or software 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.

APPENDIX E

U.S. NRC ENDORSEMENT OF STANDARDS/GUIDANCE DOCUMENTS RELATIVE TO DIGITAL COMMUNICATIONS

Standards/Guidance Document	NRC Endorsement
EWICS TC7 European Workshop on Industrial Computer Systems: "Guideline on Achieving Safety in Distributed Systems"	No endorsements found
IAEA-TECDOC-1066 "Specification of Requirements for Upgrades Using Digital Instrumentation and Control Systems"	No endorsements found
IEEE Std. 323-2003 (Rev. of IEEE Std. 323-1983) "IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations"	1. Regulatory Guide 1.209, "Guidelines for Environmental Qualification of Safety-Related Computer-Based Instrumentation and Control Systems in Nuclear Power Plants" (Formerly Draft Regulatory Guide DG-1142). ML070190294 2. NUREG-0800—Chapter 7, Appendix 7.1-B, Revision 5, Guidance for Evaluation of Conformance to IEEE Std. 279, dated March 2007 ML070550087 3. SECY-04-0109, "Final Rulemaking To Add New Section 10 CFR 50.69, "Risk-Informed Categorization And Treatment Of Structures, Systems, And Components For Nuclear Power Reactors"
IEEE Std. 603-1998 "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations"	1. Regulatory Guide 1.152, Rev. 2, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants" (Draft was issued as DG-1130, dated December 2004). ML053070150 2. Regulatory Guide 1.206, Section C.I.7, Instrumentation and Controls (Document Comparison), to Combined License Applications for Nuclear Power Plants (LWR Edition). ML070630011 3. NUREG/CR-6901 "Current State of Reliability Modeling Methodologies for Digital Systems and Their Acceptance Criteria for Nuclear Power Plant Assessments." ML060800179 4. Regulatory Guide 1.153, Rev. 1, "Criteria for Safety Systems" ML003740022
IEEE Std. 7-4.3.2-2003 "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations"	The annex is not endorsed by NRC. 1. Regulatory Guide 1.152, Rev. 2, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants" ML053070150 2. Regulatory Guide 1.209, "Guidelines for Environmental Qualification of Safety-Related Computer-Based Instrumentation and Control Systems in Nuclear Power Plants" ML070190294 3. NUREG-0800, Standard Review Plan, Chapter 7 "Review Process for Digital Instrumentation and Control Systems" ML070660258 4. SECY-08-0107, Information Report, July 28, 2008 ML082130357 5. DI&C-ISG-04, Interim Staff Guidance, Digital Instrumentation and Control. Task Working Group #4 ML072540138 6. Regulatory Guide 1.206—Combined License Applications for Nuclear Power Plants (Draft issued as DG-1145) June 2007, C. Regulatory Position Part I ML070630011

Standards/Guidance Document	NRC Endorsement
ANSI/IEEE Std. 796-1983 "IEEE Standard Microcomputer System Bus" (1988 Withdrawn Standard)	1. NUREG-1512, Vol. 1-3, "Final Safety Evaluation Report Related to Certification of the AP600 Standard Design", 1998-09-30 ML081020331 2. NUREG/CR-6303, "Methods for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems" ML071790509
IEC 60880-2006 "Nuclear Power Plants—Instrumentation and control systems important to safety—Software aspects for computer-based systems performing Category A functions"	No endorsements found
IEC 61000 "Electromagnetic Compatibility"	1. Regulatory Guide 1.180, Rev. 1, "Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems", October 2003 ML032740277 2. NUREG 0800, Standard Review Plan, Appendix 7.1-A, Second Revision 5, March 2007 (endorses RG 1.180) 3. SECY-02-0162, "SECY-02-0162 Weekly Information Report—Week Ending August 30, 2002"
IEC 61158 "Digital data communications for measurement and control—Fieldbus for use in industrial control systems"	No endorsements found
IEC 61226-2005 "Nuclear Power Plants—Instrumentation and Control Systems Important to Safety—Classification of Instrumentation and Control Functions"	No endorsements found
IEC 61513 "Nuclear power plants—Instrumentation and control for systems important to safety—General requirements for systems"	No endorsements found
IEC 61500 "Nuclear power plants—Instrumentation and control systems important to safety—Functional requirements for multiplexed data transmission"	No endorsements found
IEC 61508 "Functional safety of electrical/electronic/programmable electronic safety-related systems (E/E/PES)"	No endorsement; however, the document was reviewed. 1. SECY-05-0068—Attachment 2—Risk-Informed Regulation Implementation Plan ML050840485, 2005-04-22 2. SECY-06-0217—Enclosure 3—Risk-Informed Regulation Implementation Plan 2006-10-25 ML062650365
IEC 61511 "Functional safety—Safety instrumented systems for the process industry sector"	No endorsement; however, the document was reviewed. 1. SECY-05-0068—Attachment 2—Risk-Informed Regulation Implementation Plan, 2005-04-22 ML050840485 2. SECY-06-0217—Enclosure 3—Risk-Informed Regulation Implementation Plan 2006-10-25 ML062650365

Standards/Guidance Document	NRC Endorsement
IEC 61784-3 "Industrial communication networks—Profiles—Part 3-3: Functional safety fieldbuses—Additional specifications for CPF 3"	No endorsements found
IEC 62443 "Industrial communication networks—Network and system security—Part 1: Terminology, concepts and models"	No endorsements found
Federal Information Processing Standards (FIPS) 140-2 (Level 2)	1. Regulatory Issue Summary 2002-15 ML022400435 2. Federal Register Notice EA-08-161, 06/18/2008 ML081330420
Military Standard MIL-STD-461E "Requirements For The Control Of Electromagnetic Interference Characteristics Of Subsystems And Equipment"	Regulatory Guide 1.180, Rev. 1, Oct. 2003 "Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems", October 2003 ML032740277
VTT Research Notes 2265 "Safety of Digital Communications in Machines"	No endorsement found

APPENDIX F
NETWORK COMMUNICATION TIMING (Ref. F.1)

The timing issue focuses on the timing of the messages and transactions taking place over the system. A basic issue is whether information will be transmitted as it becomes available or transmitted periodically. Another concern is whether a message will be delivered within the allowed delay after transmission.

Event vs State Timing

These two models often used for designing control systems have their counterparts in data communication. The event model can be considered as asynchronous system design, and the state model can be described as synchronous system design. A system designed to the event model will transmit information on availability basis. On the other hand, a state model system communicates "states" at regular periods. "State" is the entire set of data shared between the communications whether the data have changed or not. For state-based system, data load on the communication link is constant, which results in fixed bandwidth use for all time. This method, however, will not use the bandwidth optimally. An event-based system transmits information depending on the availability of new information. This will use the bandwidth efficiently. However, the link can be overloaded or congested because of the variability.

Determinism, Throughput, and Delay

Determinism is important for communication systems used in real-time safety applications. A deterministic communication system delivers messages with a finite, predictable time delay that is a function of system communication load. Many communication systems are nondeterministic in nature with nonzero probability of bit error. If sufficient time delay is allowed, however, the performance of the nondeterministic system can approach the frame/packet error rate. A nondeterministic communications system of light loading and with longer permissible delays performs close to a deterministic system.

Throughput is the actual data rate successfully accomplished by the receiver. There is a relation between throughput, offered load (i.e., amount of information needed to be transmitted), and the message delay. Nondeterministic systems exhibit increasing throughput and delay with the increasing offered load. Deterministic systems show increasing throughput and moderately increasing delay that is a predicable function of the offered load.

Reference

F.1. Lawrence Livermore National Laboratory, *Data Communications*, NUREG/CR-6082, July 1993.

APPENDIX G

ADDITIONAL REVIEW INFORMATION FROM *SAFETY OF DIGITAL COMMUNICATIONS IN MACHINES*

This section of the Appendix briefly describes the VTT Research Notes 2265 document issued in October 2004 entitled *Safety of Digital Communications in Machines*, by J. Alanen et al. The document was written to bring together several international standards on safety digital communications for numerous industrial systems that have safety-critical needs. The addition of digital communications to safety systems requires supplementary components and functionality to process messages that otherwise would have been hardwired. These additional items include communication media, connectors, transceiver circuitry, communications software (and firmware), and relative and absolute time access. The VTT report discusses the issues and provides guidance for design systems to cope with communication threats and their consequences. One of the recommended features is a safety layer on top of the nontrusted communication network.

The report lists communication threats from EN 50159-2 (Refs. G.1, G.2) and adds three new threats. These are shown in Table G.1. The highlighted rows in the table indicate new errors not described in EN 50159-2.

The report describes a cause-consequence model for communications-related errors as shown in Fig. G.1. Defenses against error threats are grouped according to whether they are acting at the root-cause, message, architectural, or application-specific levels. The report provides procedural flow charts to illustrate a safety analysis methodology. The charts are shown in Fig. G.2 and Fig. G.3.

Table G.1. Communications errors extracted from VTT Research Notes 2265

Threat	Description
Repetition	Duplication, replication, or Babbling Idiot
Deletion	All or only part of the messages or part of the message content disappear
Insertion	Incorrect messages, for example, data from wrong source
Incorrect Sequence	Failure in event ordering of messages, for example, due to priority inversion
Corruption	Data word is incorrect value
Delay	Too long latencies
Messages Too Early	Prior to expected time slot, unexpected, and may be rejected or misinterpreted
Excessive Jitter	Message misses time slot, may be quarantined
Masquerade	Mixing safety-related message with nonsafety related; authentication error
Inconsistency	Two or more receivers may have inconsistent view of the transmitted data, or receivers may be in different states

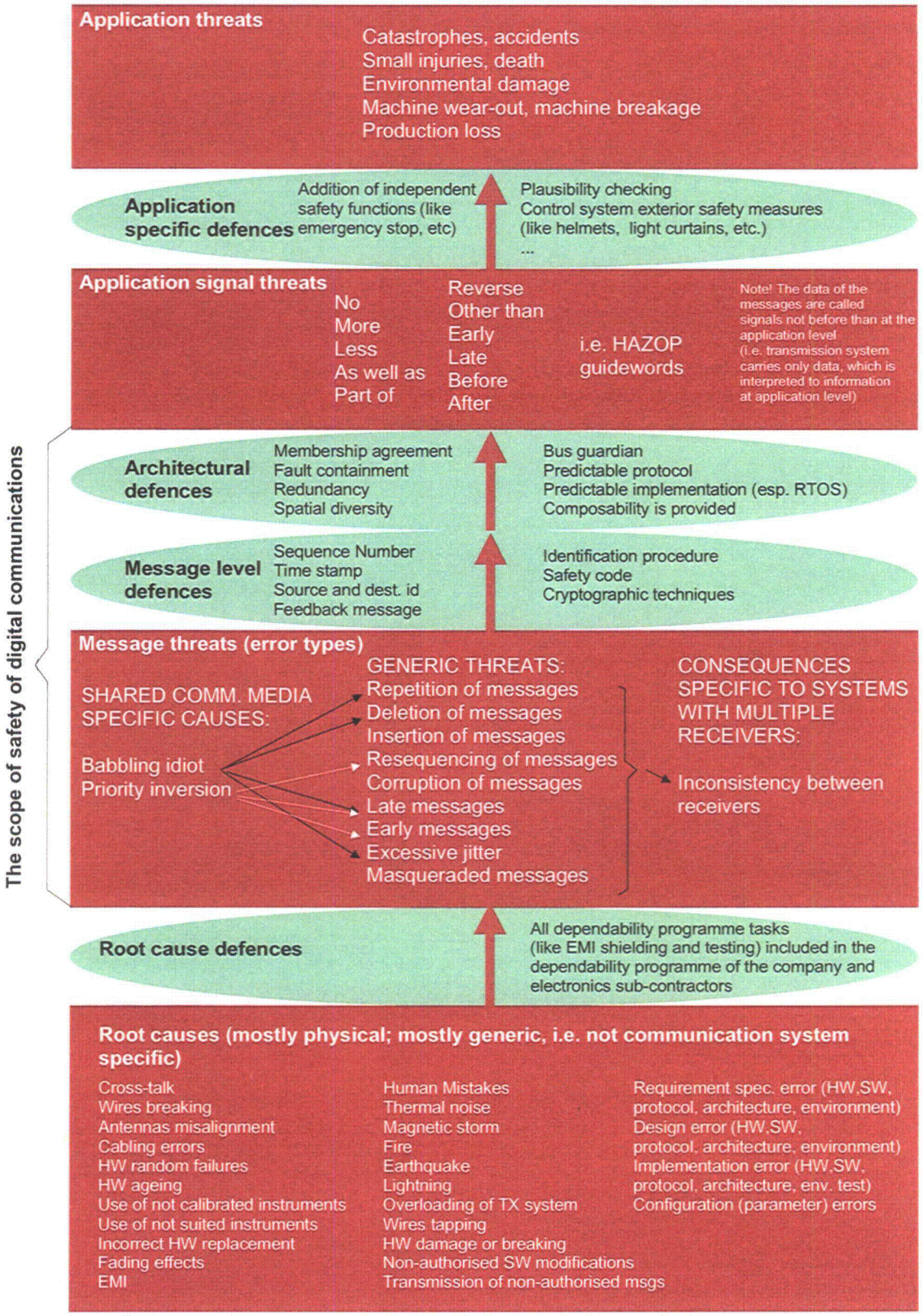

Fig. G.1. Cause-consequence model for communication-related errors. *Source*: J. Alanen et al., "Safety of Digital Communications in Machines," VTT Research Notes 2265, October 2004. Permission to use this copyrighted material is granted by J. Alanen.

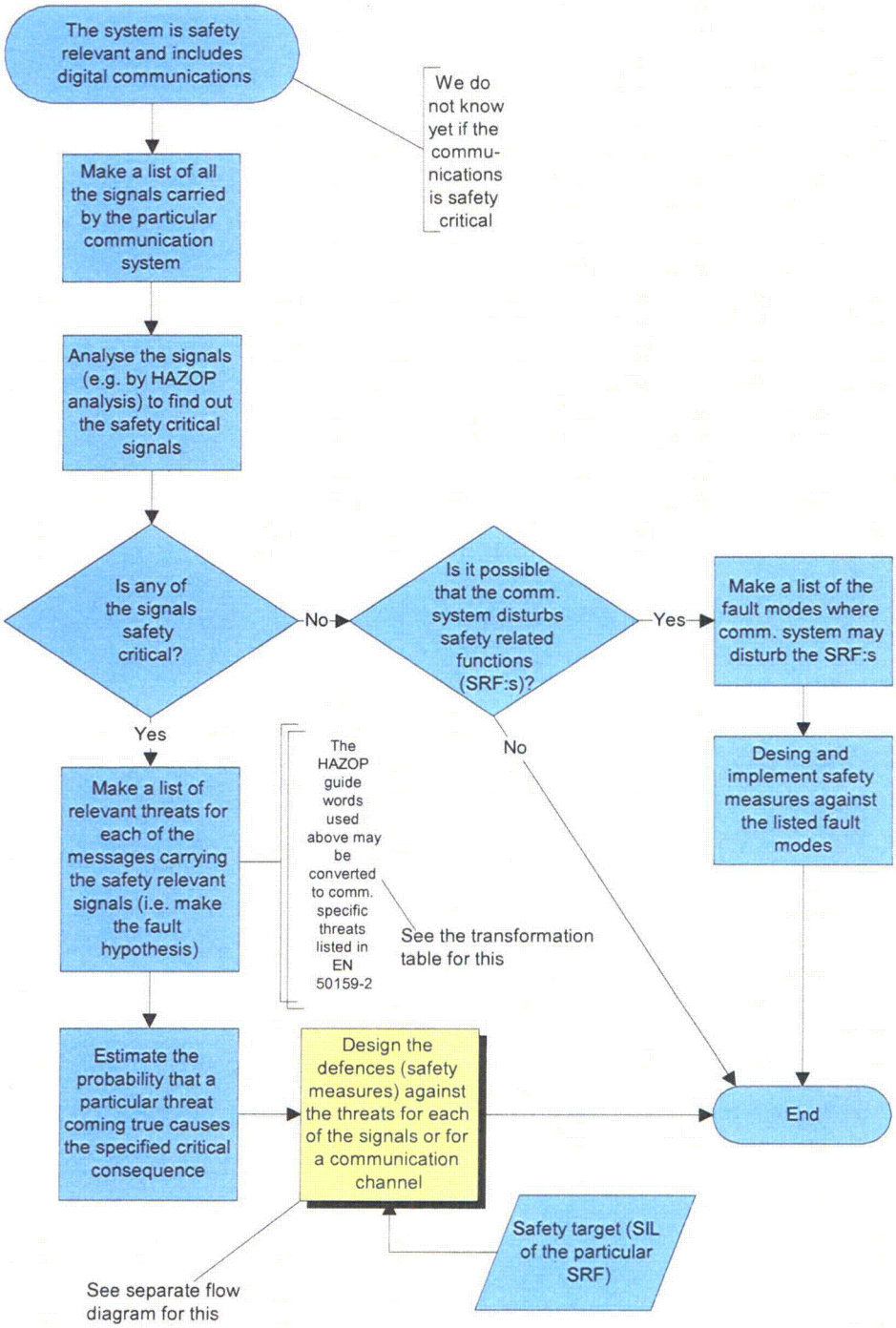

Fig. G.2. Flow chart illustrating safety analysis of digital communications network. *Source*: J. Alanen et al., *Safety of Digital Communications in Machines*, VTT Research Notes 2265, October 2004. Permission to use this copyrighted material is granted by J. Alanen.

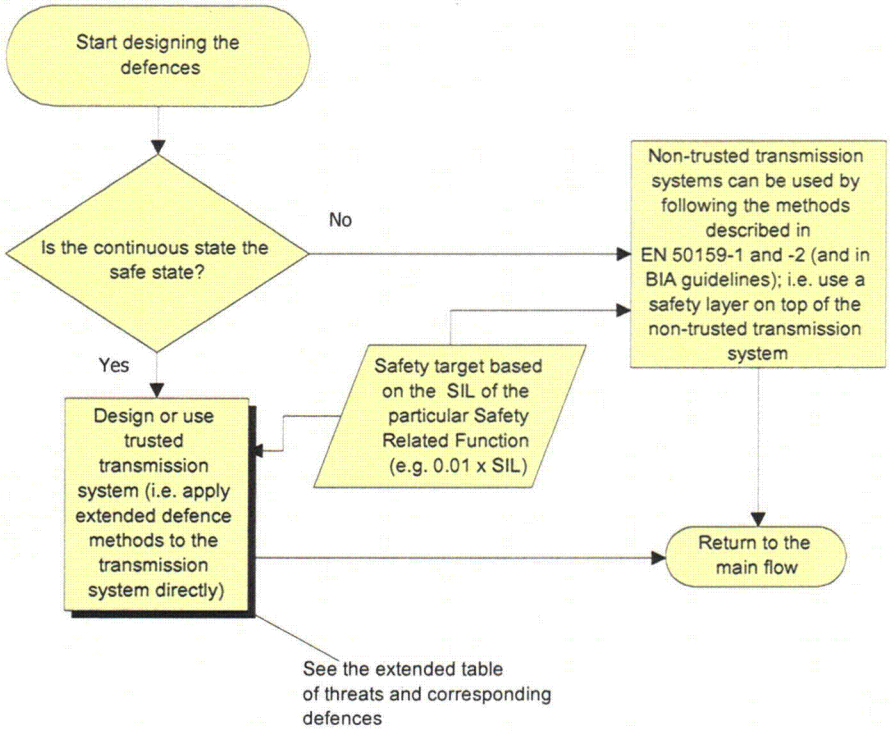

Fig. G.3. Detail of design section of analysis flow chart. *Source*: J. Alanen et al., *Safety of Digital Communications in Machines*, VTT Research Notes 2265, October 2004. Permission to use this copyrighted material is granted by J. Alanen.

Defense methods against data integrity threats are discussed in the report. Basic information on several commercial safety buses and standards to be considered during system design are covered. These are listed below:

- DeviceNet Safety
- PROFIsafe
- CANopen Framework for Safety-Relevant Communication
- EsaLAN
- SafetyBUS p
- AS-interface Safety at Work
- Interbus Safety
- TTP/C
- TTCAN
- FlexRay
- SAFELOC
- SafeEthernet

A documentation and analysis tool is also described in the report. The report applies several international standards to safety bus design. For example, the layered architecture model of EN 50159-1 is described (an example for closed transmission systems is shown in Fig. G.4).

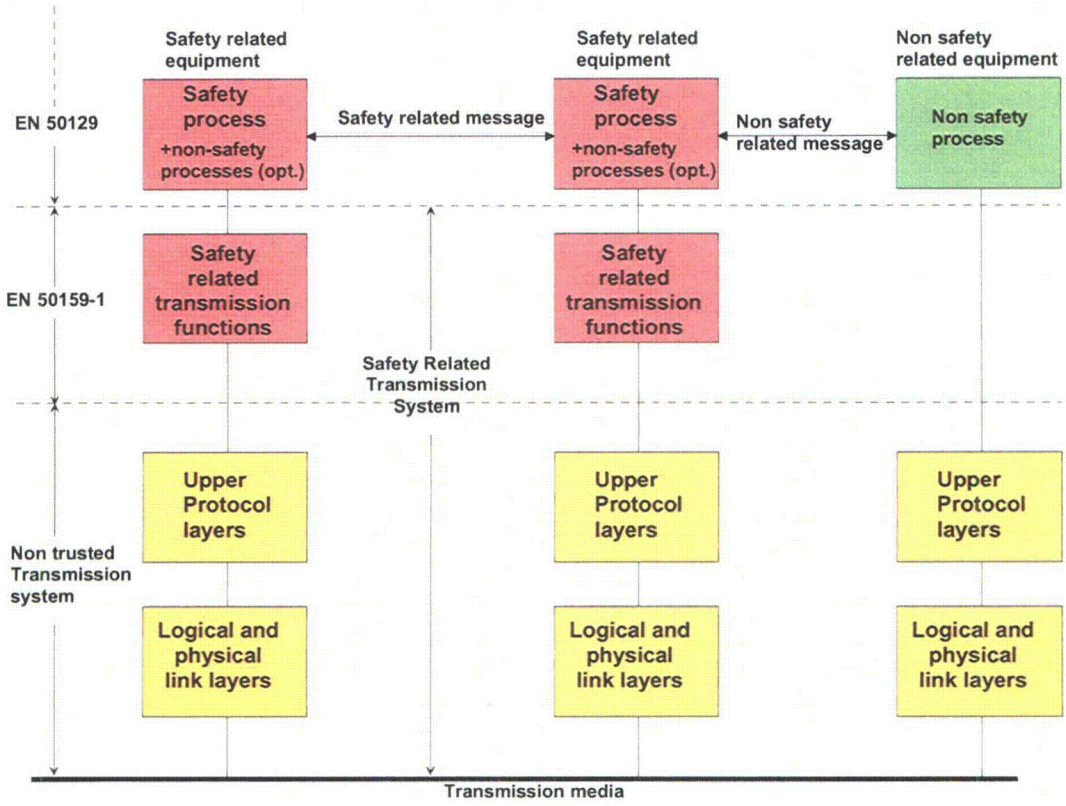

Fig. G.4. Communication model using nontrusted closed transmission system. *Source*: J. Alanen et al., *Safety of Digital Communications in Machines*, VTT Research Notes 2265, October 2004. Permission to use this copyrighted material is granted by J. Alanen.

References

G.1. EN 50159-2, "Railway Applications, Communications, Signaling, and Processing Systems," Part 1: Safety-related communication in closed transmission systems, Brussels, European Committee for Electrotechnical Standardization (2001).

G.2. EN 50159-2, "Railway Applications, Communications, Signaling, and Processing Systems," Part 2: Safety-related communication in open transmission systems, Brussels, European Committee for Electrotechnical Standardization (2001).

APPENDIX H
ADDITIONAL REVIEW AND ANALYSIS GUIDELINES

The document, "Guideline on Achieving Safety in Distributed Systems," edited by Stuart Anderson and Janusz Górski (February 2002) is a working group consensus product of the European Workshop on Industrial Computer Systems Technical Committee 7 (Safety, Reliability, and Security). The guideline concentrates on safety-critical distributed systems, that is, on the systems that may have catastrophic consequences to their embedding environments. Guidelines that pertain to the design and review of safety-related digital communication systems have been extracted with little editing from the larger collection of guidelines found in the actual document. Some of the guidelines have direct application to digital networks, while others are more indirect such as a recommendation for FMEAs of processors that may interact through the communications network. The guidelines are grouped in six categories that are life cycle oriented: Safety Analysis Guidelines, System Design Guidance, Hardware Design Guidance, Integration Guidance, Maintenance and Modification, and Security. These communication-specific guidelines are presented here without comment.

Safety Analysis Guidelines

- When distributed system components are allocated, different SILs analysis should cover whether communication with components having low SILs can compromise the SILs of more critical components.
- The analysis of synchronization hazards should consider: predictability of update time, real-time response, switchover time for redundant components.
- Check if redundancy and diversity are used adequately to avoid single points of failure and common cause failures in the communications network.
- The system specification should be analyzed to be aware of the processor task loading limits and how the system performs as loading limits are approached and passed.
- Analyze failure modes of processors under loading.
- Analyze failure modes of communication links under loading.
- Analyze hazards in configuration control.
- Analyze hazards in accesses to shared memory.
- Zonal analysis, in which the loss of all equipment in a particular location will include consideration of loss of parts of the distributed system, should be carried out to establish the effect of a loss of those parts on the functioning of other parts of the system, and hence on external systems and users. Zonal analysis is a particular case of common-cause-failure analysis, which should be carried out to establish the effects of failure of shared elements; in distributed systems, network hardware and software can provide a common failure mechanism. Typical sources of common cause failures are power supply, electromagnetic field, physical catastrophe, design errors, human training, and operating procedures.

System Design Guidance

- All operational states, including maintenance, disturbances, failure, etc., should be considered while deciding on the communications structures for the system.
- Protection measures against uncontrolled modification, adequate to the safety integrity level of a function, should be planned and implemented.
- Authorization levels in access to the system should be defined.
- Achieving satisfactory evidence that functions achieve required safety integrity level can be

enabled by (1) use of simple synchronization methods for the components realizing safety functions, for example, polling, nonpreemptive deterministic scheduling, synchronous communication, and (2) application of the "design for monitoring" principle—ensuring that all communications can be observed.

- Identify the risk associated with communication failure. Choose medium on basis of acceptable risk.
- It is important that basic design requirements for protection subsystems, control subsystems, and monitoring subsystems are not compromised by incorporating such subsystems within a distributed system network. Such basic requirements may include for instance
  — safety channel segregation (physical, geographical, electrical),
  — fail-safe design,
  — on-line maintainability, and
  — layered levels of availability.
- Redundancy—the application requirements may demand high availability for some safety critical processing functions. This may require
  — redundant information storage,
  — redundant processors, and
  — redundant communication links.

Hardware Design Guidance

- No interference should be allowed between physical communication media and protection of the communication media from environmental interference.
- Each part of the system should be capable of independently detecting failure of its electronics and the communications medium connecting it with other parts of the distributed system. In the case of failure, this should be communicable or detectable by other relevant components.
- Distributed systems are reliant upon communication subsystems to interconnect. These may be serial or parallel, but all suffer from the same restrictions. Failure of all or part of a communication system will disable the transfer of data between the parts of the distributed system. These networks are therefore a common mode of failure within the safety critical system and should therefore be considered as a candidate for redundant operation irrespective of the category of the safety system. As a minimum, the networks should be duplicated and should use independent hardware and connection routes.

Integration Guidance

- It should be ensured that communication protocols may be verified to detect data corruption on communication channels or handle misleading command sequences because of timing problems.

Maintenance and Modification

- If code is distributed across communication links, the elements used for this should be at least at the same integrity level.

Security

- Logical and physical attacks have to be considered, for example, cutting a communication line (physical attack) and malicious modification of the configuration file (logical attack).
- To protect top-level safety functions from logical attacks, isolate them functionally as far as

possible reducing the communication links to a minimum.

- If communication is inevitable, implement algorithms such that communication is controlled by the system with the higher safety level using unidirectional communication only (e.g., information dissemination instead of information request and grant strategies).
- Separate communication processes with interaction to the outside of a safety-relevant system or system part from processes that run the actual safety functions.
- Avoid any kind of remote configuration. If unavoidable, use encryption technologies to secure this information transfer.
- Identify the security-relevant information flow within a distributed system.
- Try to minimize channels with security-relevant information transfer.
- Identify the threats that have to be considered.
- Design your system with these threats in mind, implementing only those communication facilities that are absolutely necessary.
- Avoid off-the-shelf software products with no information about the security measures that were applied during development and production of the product. Weaknesses there may result in severe problems from deliberate modification of code to result in malicious program behavior.

APPENDIX I
BYZANTINE GENERALS' PROBLEM

The Byzantine Generals' Problem can be expressed abstractly in terms of a group of generals of the Byzantine Army camped with their troops around an enemy city. Communicating only by messenger, the generals must agree upon a common battle plan. The Byzantine Army is preparing for a battle. A number of generals must coordinate among themselves through (reliable) messengers on whether to attack or retreat. A commanding general will make the final decision. Any of the generals, including the commander, may be traitorous, in that they might send messages to attack to some generals and messages to retreat to others in order to confuse the others.

With three generals (two generals plus the commander), no agreement is possible if one of three generals is traitorous. The general solution requires that to reach agreement with k traitorous generals require a total of at least $3k + 1$ generals. In terms of computer systems, reliable computer systems must be able to handle malfunctioning components that give conflicting information to different parts of the system. A system needs $3k + 1$ processors to achieve k fault tolerance for agreement with Byzantine Faults. In other words, to mask one faulty processor requires a total of four processors; to mask two faulty processors requires a total of seven processors; and to mask three faulty processors requires a total of ten processors (Ref. I.1).

To more easily identify the problem, concise practical definitions of Byzantine Fault and Byzantine Failure are presented here (Ref. I.2):

Byzantine Fault:	a fault presenting different symptoms to different observers
Byzantine Failure:	the loss of a system service due to a Byzantine Fault in systems that require consensus

The only way that Byzantine Generals' Failures cannot happen in a system is if there is absolutely no cooperation among redundant elements. Once cooperation is used, Byzantine Failures can occur. For example, many distributed systems have an implied system-level consensus requirement such as a mutual clock synchronization service. Failure of this service will bring the complete system down. Asynchronous approaches do not remove these problems. Any coordinated system actions will still require consensus agreement. However, other than using intrinsically reliable circuit components, the only way for implementing a reliable computer system is to use several different "processors" to compute the same result, and perform a majority vote on their outputs to obtain a single value. [The voting may be performed within the system, or externally by the users of the output (Ref. I.2)].

Fault effects must be masked until recovery measures can be taken. A majority voting architecture with a triplex or higher level of redundancy masks errors and provides spares to restore error masking after a failure. Use of redundancy, of course, is quite common in critical systems. However, managing that redundancy is supremely important (Ref. I.3).

The use of majority voting to achieve reliability is based upon the assumption that all the nonfaulty processors will produce the same output. This is true so long as they all use the same input. However, any single input datum comes from a single physical component, and a malfunctioning component can give different values to different processors. Moreover, different processors can get different values, even from a nonfaulty input unit, if they read the value while it is changing. For example, if two processors read a clock while it is advancing, then one may get the old time and the other the new time. This can only be prevented by synchronizing the reads with the advancing of the clock (Ref. I.4).

It is tempting to try to circumvent the problem with a "hardware" solution. For example, one might try to ensure that all processors obtain the same input value by having them all read it from the same wire. However, a faulty input unit could send a marginal signal along the wire—a signal that can be interpreted by some processors as a 0 and by others as a 1. There is no way to guarantee that different processors will get the same value from a possibly faulty input device except by having the processors communicate among themselves to solve the Byzantine Generals' Problem (Ref. I.4).

General Characteristics

Byzantine Faults can be caused by simple, common phenomena. In addition, the nature of Byzantine Faults allows them to propagate through traditional fault containment zones. This invalidates system architectural assumptions that do not specifically include Byzantine Problems. To illustrate these concepts, consider a digital signal that is stuck at "1/2," that is, a voltage that is anywhere between the voltages for a valid logical "0" and a valid logical "1."

Stuck at "1/2" behavior is commonly observed with complementary metal-oxide semiconductor (CMOS) bridging faults or CMOS signal path "opens" (the most common type of fault). A similar behavior can be seen in a metastable flip-flop, which oscillates rapidly between a "0" and a "1" existing in neither state long enough to exhibit a valid output voltage. Receivers downstream of these signals may interpret them as either a "0" or a "1" depending on their respective thresholds, biases, gains, and timing. These ambiguous logic levels can propagate through almost any digital circuit. In fact, a "1/2" signal can propagate through multiple stages of logic and still remain at an ambiguous level (Ref. I.2).

Although the "1/2" type of Byzantine Problem is easier to describe, the more common problems are in the time domain. These can be either on the microscale, where data-changing edges occur at the same time as sensing clock edges (i.e., the metastability problem) or on the macroscale, where an event occurs exactly at its deadline. For example, events in a real-time system must occur before a deadline. An event occurring exactly at its deadline can be seen as timely by some observers and late by other observers.

Allowing the computers to exchange data can introduce the Byzantine Generals' Problem. For majority voting to yield a reliable system, the following two conditions should be satisfied (Ref. I.4):

1. all nonfaulty, processors must use the same input value (so that they produce the same output); and
2. if the input unit is nonfaulty, then all nonfaulty processes use the value it provides as input (so that they produce the correct output).

To be certain that faulty processors can be properly identified for isolation, it is necessary to allow for every possible misbehavior. Thus, the case when a faulty processor is malicious—that it actively and intelligently attempts to hide its malfunction—must also be handled. A list of Byzantine Faults that can affect the inputs to synchronous system as well as cross-channel voting include (Refs. I.1, I.3, I.5):

- stop and restart errors;
- sending conflicting information to different destinations, thereby "confusing" the good components;
- Babbling Idiot Problem;
- intentional or intelligent malicious attacks;
- execute slowly;

- execute at a normal speed but produce erroneous values and actively try to make the computation fail; and
- any message can be corrupt and has to be decided upon by a group of processors.

In short, a Byzantine Fault is anything within a failed component's power to attempt to corrupt the system. The Byzantine Fault can result in a Byzantine Failure wherein no agreement in the outputs between any of the computers can be reached. This situation can occur if two computers get inconsistent information from the third computer (Ref. I.5).

Methods for Coping with Byzantine Faults

The systems can be designed to prevent a Byzantine Fault from causing a Byzantine Failure by

- designing a systems such that a consensus is not needed or
- preventing the fault from propagating.

The Byzantine Generals' Problem arises when a single failure propagates via the cooperative mechanisms that the NMR system uses and causes the failure of the entire NMR system. The literature suggests that the triggers of Byzantine Generals' Faults are extremely difficult to anticipate, so the best solution is to devise ways to handle the situations they would create should they happen (Ref. I.5).

Of course, a faulty input device may provide meaningless input values. All that a Byzantine Generals' Solution can do is guarantee that all processors use the same input value. If the input is an important one, then there should be several separate input devices providing redundant values. However, redundant inputs cannot achieve reliability; it is still necessary to ensure that the nonfaulty processors use the redundant data to produce the same output (Ref. I.4).

Effective methods for dealing with Byzantine Faults can be divided into three types (Ref. I.2):

- full exchange (e.g., the SIFT, FTh4P, and SPIDER architectures),
- hierarchical exchange (e.g., the SAFEbus architecture), and
- filtering (e.g., TTP star topologies). These methods can be used separately or in conjunction with each other.

The first method directly implements the exchanges described in the classical Byzantine papers and is discussed below.

It is important to note that most, if not all, of the existing solutions based on classical full-exchange techniques (e.g., SPIDER) have an instance of the filtering method* buried inside. That is, they all assume that the second round of exchange via the intermediaries is non-Byzantine and that the intermediaries have suitably filtered the data (Ref. I.2).

As a first step in addressing this issue, redundant elements are portioned into individual fault-containment regions (FCRs). An FCR is a collection of components that operates correctly regardless of any arbitrary logical or electrical fault outside the region. Conversely, a fault in an FCR cannot cause hardware outside the region to fail. Each FCR requires at least an independent power supply and clock signal. The regions may also need to be physically separated (Ref. I.3).

Although an FCR can keep a fault from propagating to other FCRs, fault effects manifested as erroneous data can propagate across FCR boundaries. Therefore, the system must provide error containment as well. The basic principle is fairly straightforward: "voting planes" mask errors at

*"Byzantine Fault filters in the communication paths convert Byzantine signals into non-Byzantine signals.

different stages in a fault-tolerant system. For example, a typical embedded control application involves three steps: read redundant sensors, perform control law computation, and output actuator commands (Ref. I.3).

In an embedded application, an input voting plane masks failed sensor values to keep them from propagating to the control law. Internal computer voting masks erroneous data from a failed channel to prevent propagation to other channels. Output voting and an interlock mechanism prevent outputs of failed channels from propagating outside the computational core (Ref. I.3).

The Multi-Microprocessor Flight Control System (M^2FCS) was developed by Honeywell Labs during the late 1970s. The system pioneered the concept of a complete self-checking pair architecture. M^2FCS utilized a dual self-checking pair bus distribution topology (total 4 busses) between nodes of fail-silent, self-checking processing boards. The system's self-checking pair comparisons of processors, bus transmission, and bus reception enabled the precise detection of Byzantine Faults and the ability to differentiate them from other classes of faults (Ref. I.2).

Failure Modes and Effects

In a traditional system Failure Modes and Effects Analysis (FMEA)-based approach to achieving the requisite failure rate, likely failure modes of the system are analyzed, their likely extent and effects are predicted, and suitable fault-tolerance techniques are developed for each failure mode that is considered to possess a reasonable chance of occurring. If the maximum allowable probability of failure of a digital computer is 10^{-9}/h and the system must be constructed of replicated channels, each of which has an aggregate failure probability of 10^{-4}/h, it is necessary that the likelihood of a failure occurring that was not predicted and planned for must be less than 10^{-5}* (Ref. I.3).

Historical Occurrences of Byzantine Failures

Time-Triggered Architecture

The time-triggered architecture (TTA) is a generic time-triggered computer architecture for fault-tolerant distributed real-time systems. Developed from more than 20 years of research, TTA is targeted to address the needs of the emerging automotive "by-wire" industry. The dominant Byzantine Failure mode observed by Driscoll et al. (Ref. I.2) was due to marginal transmission timing. Corruptions in the time-base of the fault-injected node led it to transmit messages at periods that were slightly-off-specification (SOS); that is, slightly too early or too late relative to the globally agreed-upon time base. A message transmitted slightly too early was accepted only by the nodes of the system having slightly fast clocks; nodes with slightly slower clocks rejected the message. Even though such a timing failure would have been tolerated by the Byzantine tolerant clock synchronization algorithm, the dependency of this service on TTP/C's† membership service prevented it from succeeding. After an erroneous Byzantine transmission, the membership consensus logic of TTP/C prevented nodes that had different perceptions of this transmission's validity from communicating with each other. Therefore, following such a faulty transmission, the system partitioned into two sets or cliques—one clique containing the nodes that accepted the erroneous transmission and the other clique comprising the nodes that rejected the transmission (Ref. I.2).

---

*For the system to meet the reliability requirement, the probability that any given fault is not covered must be less than $10^{-9}/10^{-4} = 10^{-5}$.

†Deterministic fault tolerant communications protocol: TTP/C.

Quad-Redundant Control System

Consider a system comprised of quad-redundant processing elements that act on shared data collected by remote data concentrators (DCs). Each DC communicated via its own dedicated bus. On first examination, the system shows that it has sufficient fault containment zones and communication parts to tolerate a Byzantine Fault. However, there was no exchange between the processing elements. The data were used from the data concentrators as is. It was initially assumed that all processing would receive the same data, as they were connected to the same source (Ref. I.2).

This system failed because of a Byzantine Fault that was caused by an incorrect termination resistance on one of the DC-to-processor links. This bad termination caused reflections on one of the data concentrator buses. The processing elements were located at nodes and antinodes of the reflected interference and received different message values. This situation resulted in a 2:2 split of the digital redundancy that forced the system offline, leaving an independent fifth backup processor as the only operational unit.

The above example also illustrates the dangers of Byzantine Fault propagation that may invalidate the system failure assumptions—the loss of a single termination resulted in the complete loss of the digital system redundancy. As with the previous examples, the fault that led to the SOS manifestation was hard, and the SOS condition persisted.

Potential Large Economic Impact Example

If a system is not originally designed to tolerate Byzantine Faults, ensuing accidents or recalls due to their occurrence can be very expensive. The possible economic impact is illustrated in an incident where Byzantine Failures threatened to ground all of one type of aircraft. This aircraft had a massively redundant system (theoretically, enough redundancy to tolerate at least two Byzantine Faults). However, no amount of redundancy can succeed in the event of a Byzantine Fault unless the system has been designed specifically to tolerate these faults. In this case, each Byzantine Fault occurrence caused the simultaneous failures of two or three "independent" units (Ref. I.2).

Conclusions

It would appear that because existing critical computing systems are typically designed to be triply or quadruply redundant, meeting the requirements for Byzantine Resilience would require a simple rearrangement of the channels and addition of a few interchannel communication protocols.

When attempting to employ design diversity, it is critical not to defeat the benefits of bit-wise exact-match Byzantine Resilience. It is equally critical not to confuse faults in the diverse redundant application software with faults in the redundant hardware. When redundant hardware and/or software elements are implemented using different designs, bit-wise exact consensus cannot be guaranteed between the outputs of redundant processors.

With a simple voting scheme, to tolerate m Byzantine Faults requires $2m + 1$ components; three processors are sufficient to mask the fault of one of them. However, this is not the case for agreement! With three processors, agreement cannot be achieved if one of them is faulty (with Byzantine behavior). Preventing a Byzantine Failure requires the following conditions:

- *$N = 3m + 1$ FCRs,*
- *FCRs must be interconnected through $2m + 1$ disjoint paths,*
- *Inputs must be exchanged $m + 1$ times between FCRs,*
- *FCRs must be synchronized to bounded skew,* and
- *A simple TMR majority voter circuit is not Byzantine Resilient.*

The overhead for these interactive consistency algorithms can be considerable. The number of messages required to obtain interactive consistency is of the order of N^{m+1} (Ref. I.3).

References

I.1. P. Eles, "Fault Tolerance," Distributed Systems, http://www.ida.liu.se/~TDDB37/lecture-notes/lect1.frm.pdf.

I.2. K. Driscoll, B. Hall, M. Paulitsch, P. Zumsteg, and H. Sivencrona, "The Real Byzantine Generals," The 23rd Digital Avionics Systems Conference, DASC 04, Salt Lake City, Utah, October 24–28, 2004.

I.3. J. H. Lala and R. E. Harper, "Architectural Principles for Safety-Critical Real-Time Applications," Proceedings of the IEEE **82**(1), January 1994.

I.4. D. Dolev, L. Lamport, M. Pease, and R. Shostak, "The Byzantine Generals," *Concurrency control and reliability in distributed systems*, Van Nostrand Reinhold Co. New York, NY, 1987.

I.5. A. Girault, C. Lavarenne, M. Sighireanu, and Y. Sorel, "Fault-Tolerant Static Scheduling for Real-Time Distributed Embedded Systems, 21st International Conference on Distributed Computing Systems, ICDCS'01, Phoenix, Arizona, April 2001.

NRC FORM 335
(9-2004)
NRCMD 3.7

U.S. NUCLEAR REGULATORY COMMISSION

BIBLIOGRAPHIC DATA SHEET

(See instructions on the reverse)

1. REPORT NUMBER
(Assigned by NRC, Add Vol., Supp., Rev., and Addendum Numbers, if any.)

NUREG/CR- 6991
(ORNL/TM-2007/184)

2. TITLE AND SUBTITLE

Design Practices for Communications and Workstations in Highly Integrated Control Rooms

3. DATE REPORT PUBLISHED

MONTH	YEAR
September	2009

4. FIN OR GRANT NUMBER

N6350

5. AUTHOR(S)

R. Kisner, D. Holcomb, J. Mullens, T. Wilson, R. Wood, K. Korsah, M. Muhlheim, A. Qualls, M. Howlader, G. Wetherington, Jr., P. Chiaro, Jr., and A. Loebl

6. TYPE OF REPORT

Technical

7. PERIOD COVERED *(Inclusive Dates)*

8. PERFORMING ORGANIZATION - NAME AND ADDRESS *(If NRC, provide Division, Office or Region, U.S. Nuclear Regulatory Commission, and mailing address; if contractor, provide name and mailing address.)*

Oak Ridge National Laboratory
Managed by UT-Battelle, LLC
Oak Ridge, TN 37831-6075

9. SPONSORING ORGANIZATION - NAME AND ADDRESS *(If NRC, type "Same as above"; if contractor, provide NRC Division, Office or Region, U.S. Nuclear Regulatory Commission, and mailing address.)*

Division of Engineering, Office of Nuclear Regulatory Research
U.S. Nuclear Regulatory Commission
Washington, DC 20555–0001

10. SUPPLEMENTARY NOTES

Paul J. Rebstock, NRC Project Manager

11. ABSTRACT *(200 words or less)*

This report presents current practices in the design of highly integrated control rooms (HICR) in nuclear power plants in other countries and in similar applications in other industries. The principal features of the HICR are extensive use of digital network communications and digital operator workstations. The purpose of this report is to support the development of guidance that specifically addresses issues related to communication among safety divisions and between safety-related equipment and equipment that is not safety related.

The report examines (1) operating experience and lessons learned, (2) accepted consensus practices, and (3) analysis of credible failure mechanisms arising from several possible network architectures and message types. 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 because of transmission errors.

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

This report presents the findings and observations that resulted from the associated research. It does not indicate NRC endorsement of the designs and methods reported. The Foreword to this report provides additional clarification of this subject.

12. KEY WORDS/DESCRIPTORS *(List words or phrases that will assist researchers in locating the report.)*

highly integrated control room, digital communcations, digital workstations, safety communication, communication errors, communication standards, communication equipment qualification, communications security, digital communications acceptance criteria

13. AVAILABILITY STATEMENT

unlimited

14. SECURITY CLASSIFICATION

(This Page)
unclassified

(This Report)
unclassified

15. NUMBER OF PAGES

16. PRICE

Federal Recycling Program