IEEE Application Guide for Distributed Digital Control and Monitoring for Power Plants

Sponsor
Energy Development and Power Generation Committee
of the
IEEE Power Engineering Society

Approved September 26, 1991

IEEE Standards Board

Abstract: Alternate approaches to applying a digital control system, for both new construction and existing plant modernization projects, are described, and their advantages and disadvantages are compared. Criteria to be used to judge the suitability of commercially available systems for use in the power generation industry are provided. Terminology is defined, and the objectives of distributed control and monitoring systems are described. The following system application issues are addressed: integrated versus segregated systems, functional and geographic distribution, hierarchical architecture and automation, control and protection functions, input/output systems, environmental considerations, and documentation. The data communications structure and the functions that support it are considered. Data acquisition and monitoring (the man/machine interfaces) are discussed. Reliability, availability, and fault tolerance of distributed control and monitoring systems are addressed.
Keywords: Power plant, control, distributed control, digital, monitoring, distributed monitoring

The Institute of Electrical and Electronics Engineers, Inc.
345 East 47th Street, New York, NY 10017-2394, USA

Copyright © 1991 by The Institute of Electrical and Electronics Engineers, Inc.
All rights reserved. Published 1991
Printed in the United States of America

ISBN 1-55937-106-4

No part of this publication may be reproduced in any form, in an electronic retrieval system or otherwise, without the prior written permission of the publisher.

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS
Not for Resale

IEEE Standards documents are developed within the Technical Committees of the IEEE Societies and the Standards Coordinating Committees of the IEEE Standards Board. Members of the committees serve voluntarily and without compensation. They are not necessarily members of the Institute. The standards developed within IEEE represent a consensus of the broad expertise on the subject within the Institute as well as those activities outside of IEEE which have expressed an interest in participating in the development of the standard.

Use of an IEEE Standard is wholly voluntary. The existence of an IEEE Standard does not imply that there are no other ways to produce, test, measure, purchase, market, or provide other goods and services related to the scope of the IEEE Standard. Furthermore, the viewpoint expressed at the time a standard is approved and issued is subject to change brought about through developments in the state of the art and comments received from users of the standard. Every IEEE Standard is subjected to review at least once every five years for revision or reaffirmation. When a document is more than five years old, and has not been reaffirmed, it is reasonable to conclude that its contents, although still of some value, do not wholly reflect the present state of the art. Users are cautioned to check to determine that they have the latest edition of any IEEE Standard.

Comments for revision of IEEE Standards are welcome from any interested party, regardless of membership affiliation with IEEE. Suggestions for changes in documents should be in the form of a proposed change of text, together with appropriate supporting comments.

Interpretations: Occasionally questions may arise regarding the meaning of portions of standards as they relate to specific applications. When the need for interpretations is brought to the attention of IEEE, the Institute will initiate action to prepare appropriate responses. Since IEEE Standards represent a consensus of all concerned interests, it is important to ensure that any interpretation has also received the concurrence of a balance of interests. For this reason IEEE and the members of its technical committees are not able to provide an instant response to interpretation requests except in those cases where the matter has previously received formal consideration.

Comments on standards and requests for interpretations should be addressed to:

Secretary, IEEE Standards Board
445 Hoes Lane
P.O. Box 1331
Piscataway, NJ 08855-1331
USA

IEEE Standards documents are adopted by the Institute of Electrical and Electronics Engineers without regard to whether their adoption may involve patents on articles, materials, or processes. Such adoption does not assume any liability to any patent owner, nor does it assume any obligation whatever to parties adopting the standards documents.

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS
Not for Resale

Foreword

(This Foreword is not part of IEEE Std 1046-1991, IEEE Application Guide for Distributed Digital Control and Monitoring for Power Plants.)

At the IEEE Winter General General Power meeting in 1984, the Power Plant Protection, Plant Protection Control, and Automation Subcommittee proposed that a working group be established to analyze the power plant application problems raised by the rapid progression in the technology of distributed digital control. Dr. D. J. Damsker was appointed to be the Chairman of the Working Group for the development of this guide document.

Distributed digital control and monitoring systems have become increasingly accepted and used in all industrial fields; however, power generation has its specific characteristics and requirements. It is these specifics that this guide attempts to address.

This guide is dedicated to establishing advanced features for distributed control and monitoring systems for power plants. The special requirements for nuclear generating plants are beyond the scope of this document. The basic principles and control philosophy developed in this guide can apply to any kind of distributed digital control for non-nuclear power plants, but only the specific control aspects of fossil-fuel power plants have been addressed (e.g., no details of hydroelectric power plants have been considered).

The integrated control strategy of a power plant now involves and requires the use of structured software to be adequately supported by a distributed hardware architecture. Links with management integrated software (MIS) can impose even more conditions on the control computer network.

The data communications structure (the control data network) is still under development and has not yet reached its ultimate technological stage. The power plant control, safety, dependability, quality of performance, the processing of sophisticated programs (such as expert systems) and their integration into distributed control systems all depend on how well the network architecture problems have been solved.

The first purpose of this document is to define the required terminology in order to establish both common and correct usage.

Other purposes of IEEE Std 1046-1991 include:

- The advancement of the common practice and technological state of the art;
- The increase of power plant availability, controllability, efficiency, and load demand;
- The decrease of investment, operation, and maintenance costs.

Criteria of functional and geographical computer distribution are established. Hierarchical considerations and automation of control and network architecture are analyzed and best solutions are suggested.

IEEE Std 1046-1991 attempts to take into account all aspects of power generation requirements, as the basis for establishing application criteria of distributed digital control and monitoring systems.

The membership of the Working Group during the preparation of this document was:

D. J. Damsker *(Chairman, Working Group)*
A. Leus *(Chairman, Working Section)*
W. J. Spengel, *Secretary*

P. A. Babonis
J. W. Bayless, III
G. B. Fasset
L. E. Fennern
D. E. Hamme
J. A. Kamel
J. A. Kopczynski
J. F. McConlogue
D. Rice
J. A. Schuss
J. R. Short
R. C. Szczerbicki
M. Salm

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS
Not for Resale

The following persons were on the balloting committee that approved this document for submission to the IEEE Standards Board:

I. B. Berezowsky
S. R. Brockschink
R. L. Castleberry
E. F. Chelotti
R. S. Coleman
R. E. Cotta
M. L. Crenshaw
D. J. Damsker
G. Engmann
A. H. Ferber
W. W. Fields
D. I. Gorden
J. H. Gurney
T. J. Hammons
R. D. Handel
C. E. Hickman
M. E. Jackowski
J. H. Jones
P. R. H. Landrieu
J. E. LeClair
G. L. Luri
J. T. Madill
O. S. Mazzoni
D. R. McCabe
G. R. Meloy
J. L. Mills
C. R. Pope
E. P. Rothong
J. E. Stoner, Jr.
R. E. Strasser
T. R. Whittemore
J. P. Whooley

When the IEEE Standards Board approved this standard on September 26, 1991, it had the following membership:

Marco W. Migliaro, *Chair*
Don Loughry, *Vice Chair*
Andrew G. Salem, *Secretary*

Dennis Bodson
Paul L. Borrill
Clyde Camp
James M. Daly
Donald C. Fleckenstein
Jay Forster*
David F. Franklin
Ingrid Fromm
Thomas L. Hannan
Donald N. Heirman
Kenneth D. Hendrix
John W. Horch
Ben C. Johnson
Ivor N. Knight
Joseph L. Koepfinger*
Irving Kolodny
Michael A. Lawler
Donald C. Loughry
John E. May, Jr.
Lawrence V. McCall
Donald T. Michael*
Stig L. Nilsson
John L. Rankine
Ronald H. Reimer
Gary S. Robinson
Terrance R. Whittemore

Christopher J. Booth
IEEE Standards Project Editor

* Member Emeritus

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS
Not for Resale

CLAUSE PAGE

1. Scope and Purpose 1

1.1 Introduction 1
1.2 Scope 2
1.3 Purpose 4

2. Terminology and Definitions 5

2.1 Introduction 5

3. Objectives of Distributed Control and Monitoring Systems 10

3.1 Introduction 10
3.2 Dependability 10
3.3 Plant Efficiency 10
3.4 Improved Response Time 11
3.5 Extended Equipment Life 11
3.6 Improved Operation 11
3.7 Improved Operator Interface 11
3.8 Accessibility of Plant Data 12
3.9 Cost-Related Factors 12

4. System Application Issues 12

4.1 Introduction 12
4.2 Integrated vs. Segregated Systems 14
4.3 Functional and Geographic Distribution 16
4.4 Hierarchical Architecture and Automation 19
4.5 Control and Protection Functions 23
4.6 Input/Output System 28
4.7 Environmental Considerations 30
4.8 Documentation 33

5. Data Communications Structure 35

5.1 Scope and Purpose 35
5.2 Data Communication Functions 36
5.3 Data Communication Structure Characteristics 36
5.4 Control Data Communication Requirements 40
5.5 Control Data Communications Assessment 46

6. Network Architectural View 47

6.1 Introduction 47
6.2 Remote Intelligence of Distributed Control Systems 48
6.3 Single Linear Network Topology—Data Station Architecture 51
6.4 Some Special Features of Proprietary Control Networks 57
6.5 Hierarchical Network Architectures and the Field Bus 61

7. Data Acquisition and Monitoring 64

7.1 Introduction 64

--`,,```,,,,````-`-`,,`,,`,`,,`---
Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS Not for Resale

CLAUSE PAGE

7.2 Man/Process, Man/System Interfaces 64
7.3 Reporting Functions 74
7.4 Monitoring Function 75
7.5 Operating Functions 76
7.6 Diagnosing Functions 76
7.7 Plant Performance Function 79
7.8 Optimization 79
7.9 Processing 80
7.10 Data Acquisition and Preprocessing Functions 81

8. Reliability, Availability, and Fault Tolerance of Distributed Control and Monitoring Systems 81

8.1 Introduction 81
8.2 Overall View 81
8.3 Reliability 82
8.4 Software/Human/Hardware Reliability 84
8.5 Partitioning, Redundancy, and Fault Tolerance 85
8.6 Fault Tolerance 87
8.7 General Requirement for Reliability/ Availability of Distributed Control System 89
8.8 Introduction to Reliability/Availability Calculations 90

9. Bibliography 94

Annex A (Informative) Reliability and Availability 99

Annex B (Informative) FMEA/FTA Failure Mode Effect Analysis (FMEA) 111

--`,,`-`-`,,`,,`,`,,`---

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS Not for Resale

IEEE Application Guide for Distributed Digital Control and Monitoring for Power Plants

1. Scope and Purpose

1.1 Introduction

This Application Guide is to be used as an aid for the user and system designer in the proper application of distributed digital control and monitoring systems for power generating plants. This guide is dedicated to establishing advanced requirements for distributed control and monitoring systems. Topics discussed can be applied to other industries as well, but this document is addressed specifically to the requirements of the non-nuclear power generating plant. The special requirements for nuclear generating plants are beyond the scope of this document. The basic principles and control philosophy developed in this guide can apply to any kind of distributed digital control for non-nuclear power plants, but only the specific control aspects of fossil-fuel power plants have been addressed (e.g., no details of hydroelectric power plants have been considered).

Distributed control and monitoring systems can aid in maximizing plant efficiencies, availability, and reliability within the constraints imposed by the operating equipment and process cycle. With historically increasing fuel costs and the depletion of generation reserves, the importance of these improvements has become a significant issue in the utility industry.

This Guide suggests the concept of an integrated, distributed, plant-wide system performing all plant control, serving as the source of all process and equipment data, and providing services to other functional levels in a hierarchical plant automation scheme. The Guide defines criteria for selecting control and monitoring system design parameters for both new construction and existing plant modernization projects. These criteria can then be used to make intelligent and informed decisions on the specifics of any new control and monitoring system at a utility power plant.

This section of the application guide delineates the scope of the document and introduces concepts used throughout the guide.

The guide itself is organized around specific functional topics as presented in Fig 1. Figure 1 gives an architectural view of the control and monitoring task that shows the relationships among the topics discussed and notes references to the sections of the guide in which they are discussed. (*Note:* The letter "S" in the figure denotes the section of the guide that applies to that portion of the figure.)

--`,,-`-`,,`,,`,`,,`---

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS
Not for Resale

Throughout this guide the flow of information to, from, and throughout the distributed control and monitoring system is presented in semantic networks. These are flowcharts depicting tasks performed in the distributed control and monitoring system as nodes. Data paths between these nodes show the relationships among the tasks.

1.2 Scope

Digital control technology, microelectronics, and digital data communication are rapidly evolving fields. Controversial issues such as geographical and functional distribution, network topologies, hierarchical architectures, medium access control, and the physical connection are not resolved. A single design standard to cover the scope outlined above is impractical. This guide, therefore, addresses alternate approaches to the task of applying a digital control system, comparing relative advantages and disadvantages of these approaches, and addresses criteria to be used to judge the suitability of commercially available systems for use in the power generation industry.

1.2.1 Power Plant Computing Applications

Typical power plant computing functions have included the following, not all of which are addressed by this guide:

1.2.1.1 Operational Tasks

These tasks must be performed in real time. They are the link to and maintain control over the plant processes. These tasks may be classified as follows:

1) Process control
2) Process monitoring and prefault analysis
3) Human and equipment protection and safety
4) Real time performance calculations
5) Process optimization and automation
6) Fire protection

1.2.1.2 Engineering Tasks

These tasks need not be performed in real time, but interact directly with the operational tasks listed above. They are performed with the control system in service—i.e., on-line. These tasks include the following:

1) Control system optimization
2) Control system diagnostics and maintenance
3) Historical performance analysis
4) Data logging, trending, and storage

1.2.1.3 Technical Support Tasks

These tasks are not performed in real time, but are performed on-line and are distinct from operational tasks. They may require data from operational or engineering tasks, but do not generally interact with the operational tasks:

1) Plant diagnostics
2) Plant maintenance and repair
3) Plant security
4) Training/simulation
5) Plant modernization and upgrades
6) Fuel quality analysis

Copyright © 1991 IEEE All Rights Reserved

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS Not for Resale

1.2.1.4 Administrative/Management Information Systems Tasks

These are off-line tasks and are considered under the general term of management information systems (MIS). They are generally batch processed and are unrelated to plant operation. Interaction between these tasks and tasks in other categories is minimal:

1) Inventory (spare parts) control
2) Payroll and accounting
3) Forecasting, planning

1.2.2 Limits of Application Guide Scope

This Application Guide is concerned only with those functions associated with the operation of the power plant, operational and engineering tasks, not with the support services included as technical support and administrative tasks listed above. Each industry and corporation has its specific administrative and management task organizations. Even though a computerized connection among all tasks is desirable, the current technology cannot provide a standard or unique solution to such a desired goal. The MIS tasks must be separately treated from the control and monitoring tasks especially for the power industry (see Section 6). This exclusion should not be interpreted as an argument to exclude these tasks from their proper place in a multilevel data network. However, a network which is also responsible for support and administrative tasks is unlikely to be suitable for the critical control functions addressed in this Guide. It is the intention of this document to focus attention upon the unique requirements associated with the proper control of the power plant. It should be noted that there is a relationship between support and operational tasks through diagnostic messages and alarms. Field instrumentation is also excluded from the scope of this Guide; however, the interface between the field devices and the control and monitoring system I/O ports, whether hardwired to each device or through a softwired shared medium, is included. This interface is considered a part of the data communication structure and is addressed in that context. It must be noted that field instrumentation may be a limiting element for achieving performance improvement using distributed control on retrofit projects.

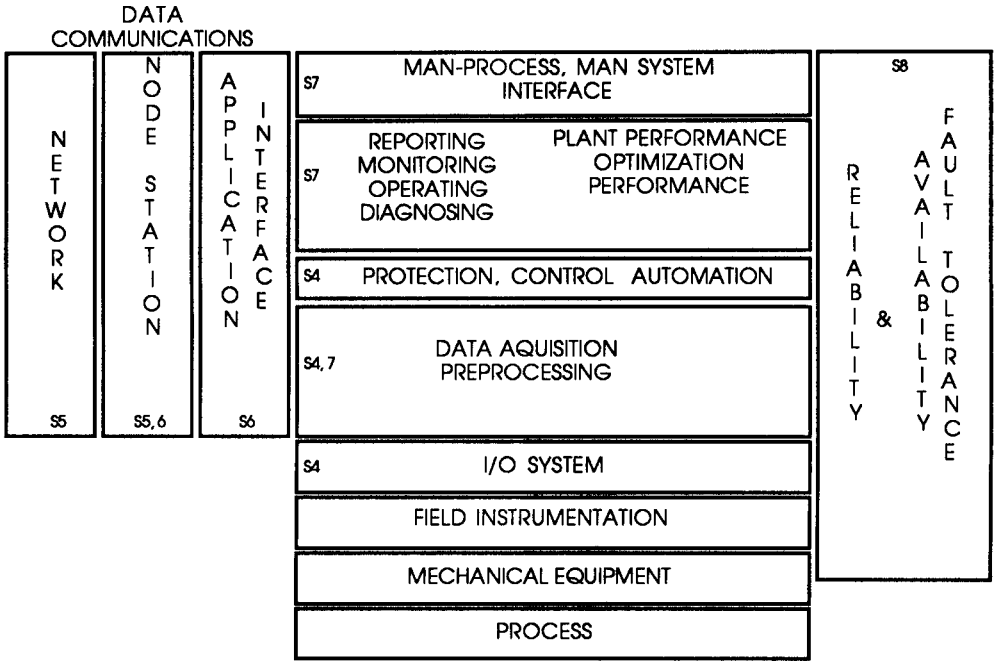


Figure 1—Architectural View of IEEE Std 1046-1991

Copyright © 1991 IEEE All Rights Reserved

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS
Not for Resale

The power plant functions included under the scope of this Guide include the control and monitoring tasks from fuel handling (e.g., coal unloading and stackout) through the transmission of electrical energy. *Note*: the switchyard is not included even though the system can be extended to include this area.

1.3 Purpose

The purpose of this application guide is to establish the following:

1) A consistent set of definitions and terminology for distributed digital control and monitoring systems (Section 2);
2) Definition of objectives and requirements for distributed systems (Section 3);
3) Practical methods and criteria to assess the performance of distributed systems as pertinent to power plant requirements Sections 4 through 8).

1.3.1 Objectives of a Distributed Control and Monitoring System

The objectives of a distributed control and monitoring system are discussed in Section 3 and include the following:

1) High plant dependability, including smaller failure rates, shorter repair and maintenance times;
2) High plant efficiencies during all modes of operation;
3) Improved response time to load changes;
4) Extended plant equipment lifetimes through reduced wear;
5) Improved safe operation through increased automation;
6) Improved operator interface to the plant;
7) Improved accessibility of plant data to engineering and management personnel.

The purpose of this document is to provide guidance to the user to help to reach these objectives in the application of distributed digital control and monitoring systems.

1.3.2 Requirements for Distributed Control Systems

The requirements for distributed systems may be organized into several categories as follows:

1.3.2.1 Safety Requirements

This Guide does not repeat or supplant any local, state, national, or international standards or codes. It does, however, address certain specific safety hazards associated with distributed control systems.

1.3.2.2 Dependability Requirements

Through features such as partitioning, distributed redundancy and fault tolerance, distributed systems are capable of attaining a higher availability than are conventional systems. Quantitative determination of reliability (in terms of MTBF) and availability can be made for distributed systems. Another component of the dependability of a system is the quality of its constituent elements, hardware and software. Section 8 of the Guide addresses all of these issues.

1.3.2.3 Performance Requirements

These are the core requirements for distributed systems and can be further subdivided as follows:

1) Functional Requirements: The specific tasks to be accomplished by the control system and acceptance criteria for each are the basis by which an application may be judged. These requirements establish guidelines against which competing systems or configurations may be compared. These requirements are discussed in Sections 4, 5, 6, and 7

Copyright © 1991 IEEE All Rights Reserved

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS Not for Resale

2) Implementation Requirements: Distributed digital hardware can be configured in many different ways. These requirements relate to the issues of functional and physical distribution, topologies, network architecture, hardwired vs. network communication for protection and alarming, etc. These issues are discussed in Sections 4 and 8
3) Integrity Requirements: Digital data communications is essential to digital control systems. Data integrity is an element of the dependability, safety, and timing of the communications structure. Network issues such as message frame format are discussed in Sections 5 and 6
4) Timing Requirements: By their nature as sequential state machines, distributed systems can only approximate real time control and monitoring. The fidelity of this approximation is a function of the degree to which the system conforms to the timing requirements for the application. Response time and information consistency are vitally important for distributed systems. Features such as distributed processing, multi-processing, etc., help to approximate real time control, but do not ensure information consistency throughout the system. Timing constraints are the basic component of "information consistency," which also includes consideration of the time period over which a value remains valid for control action (validity time) and the simultaneity of the same measured value throughout the system. Generally, the control system response time is far less than the process time, i.e., process system capacity allows the control system to have a time delay latitude. These issues are discussed in Sections 4, 5, 6, and 7 of this Guide.

2. Terminology and Definitions

2.1 Introduction

This section defines the key terms used throughout this document. At present, vendors, end users, and architect-engineers are using several terms denoting the same meaning, or a number of meanings for one term. It is the intent of this section to define one set of terms, each with a single definition, that are to be used throughout the application guide. Therefore, Section 2 becomes important to establish a common database of terms that shall be used by everyone in the electric utility industry. This common database or dictionary of terms would make communication both written and verbal, between utilities, vendors, and architect-engineers much easier.

Section 2 will establish a common mode of communication for new control and monitoring systems in the electric utility industry.

The following terms and definitions denote some of the key words that are used in this Application Guide.

adaptive control: Control action whereby automatic means are used to change the type or influence (or both) of control parameters in such a way as to improve the performance of the control system.

artificial intelligence: A branch of computer science that attempts to have a computer emulate intelligent behavior. By "intelligent behavior" is meant reasoning procedures that do not appeal to mathematical and logical computations, but to means that are used by mental reasoning, such as inferences, pattern recognitions, qualitative and quantitative estimations, and the like.

automation: The use of adequate computer capacities, such as logic controllers, sequence controllers, modulating controllers, and processors in order to bring every piece of plant equipment into operation, optimize operation in a steady state condition, and shut down the equipment in the proper sequence under set safety operating conditions.

automation hierarchy: The design and implementation of automation functions in a multilevel structure, such as local level, group level, unit level.

availability: A statistical measure of how often a system is in a condition to deliver specified service to a user under stated conditions. Availability is is expressed as a ratio between the time during which the system is able to perform its duty and the total of this time and the outage time. The availability figure is a value between 0 and 1.

Copyright © 1991 IEEE All Rights Reserved

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS Not for Resale

baseband local area network: A single-channel local area network that uses only one medium, impressing directly the signal codes on it, without frequency modulation.

bridge: A device that interconnects two compatible networks. As opposed to a repeater, a bridge selects the messages which it transfers reciprocally from one network to another.

broadband local area network: A network with a single media capable of carrying multiple modulated channels, specifically, data, voice and TV channels.

bus: A control network technology in which data stations share one single linear medium system. Messages propagate the length of the medium and are received by all data stations simultaneously.

carrier band: The sole frequency band used by a single channel local area network, when the signal is frequency modulated.

common mode failure source: An element of the control system that, when it fails, influences more than one piece of process equipment, and inhibits operation of more than one out of a group of process parts.

common practice: Constitutes the well-established technical solutions offered by more or less old technology to a given problem, applied by the majority of users.

configuration: A specific logical or physical arrangement of system equipment and fuctionality designed to meet user needs.

control: The operation of the system according to prescribed processing procedures or to operator's commands, so that the process status stays within allowed or desired state spaces.

control configuration: A configuration established for control purposes.

control cycle time: The span in which the inputs to the system are iteratively renewed.

control data network: Communications structure that conveys data throughout the system.

control hierarchy: A system organization incorporating multiple levels of control responsibility.

control logic: The control plan for a given system. The program.

control philosophy: The total concept on which a power plant control system is based.

database: The collection of stored data regarding the process variables and processing procedures.

data acquisition: That function (task) of a distributed control system (DCS) that collects, converts, or processes the raw information delivered by the field sensors in order to make available for the system a dynamic range of state variable and process events (a live image of the process dynamics).

data station: A device performing specific control functions that communicate through the node on the control network or sub-networks. Typical functions are data acquisition, monitoring, calculation, logging, controlling, printing, interfacing, etc.

dependability: A synergistic combination of reliability, availability, and quality.

distributed processing: An organizational mode of operation in which multiple processors, each with their own memory, are working concurrently, and are loosely connected by a network.

distributed redundancy: Specific redundancy that is arranged on a modular basis, is distributed rather than concentrated and applies whether or not the monitoring and control system is partitioned to follow the plant equipment redundancy.

distributed risk of failure: Distribution of functionality within a system, to allow several levels of degradation prior to the inability of a system to perform its task.

expert systems: Computer programs that embody judgmental and experimental knowledge about a computer application. Expert systems are capable of providing expert advice in some well-defined domain. Expert systems are able to reach decisions from new, uncertain and incomplete information with a specified degree of certainty. Expert systems abilities include; making logical inferences under unforeseen conditions; using subjective and formal

 Copyright © 1991 IEEE All Rights Reserved

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS Not for Resale

knowledge; explaining the procedures used to reach a conclusion; growing in effectiveness as embedded expertise is expanded and modified.

failure: Whatever course that makes the external behavior of a system not conform to the expected specified performance of a system

failure mode effect analysis (FMEA): Systematic process aimed at identification and elimination or compensation of failure modes for reliability improvement. This methodology is usually based on single failures.

fall back: A degraded system mode of operation. A fall back entails an alternate strategy to continue functioning, with partial functionality in spite of faults.

fault: Any cause within the system that brings the system to a pre-failure state.

fault tolerance: The built-in capability of a system to provide continued correct execution in the presence of a limited number of hardware or software faults.

fault tree analysis (FTA): Systematic process involving a logic diagram that describes a combination of component (module) failures that cause a top event to occur.

field bus: A digital data communications means that makes possible the exchange of information among peripheric or separate elements of a distributed control system or between such elements and other subsystems.

functional distribution: *(A) State of the art definition.* A physical distribution of programs among distinct hardware capacities, partitioned according to control functional tasks. *(B) Common practice definition.* Implementing a control loop entirely within a single station, such that neither the process data nor the control signal output to the actuator is passed through the communications networks.

functional integrity: The quality and state of a system in which all functions a system was designed to perform are available at that moment.

gateway: A device connecting two computer systems that usually use different protocols, or to connect two independent networks.

geographical distribution: A method to deploy the system in accordance with the physical layout of the plant, the minimum wiring criterion, and specific environmental distribution requirements.

hot repair: The replacement of a piece of equipment, printed circuit card, or data station while the system remains operational.

imagery techniques: The science and art of automatically presenting information by images. (Sometimes referred to as imaging.)

information consistency: A generic term that designates the extent to which the process states and events, the corresponding data used by the control system, and the corresponding information provided to the operator are in good agreement, within the same granulation time, in order for the system to bring or keep the process in the optimization range.

integrated system: A system with integrated programs processed on a local basis, based on the local availability of information, without consideration given to segregation into sub-systems.

mean time between failure (MTBF): The time interval (hours) that may be expected between failures of an operating equipment.

mean time to detection (MTTD): The elapsed time between the occurrence of a failure until it is detected by the service personnel.

mean time to repair (MTTR): The time interval (hours) that may be expected to return a failed equipment to proper operation.

measurement instrumentation: Field devices that provide information on process variables and sometimes initiate appropriate action (e.g., transmitters, thermocouples, limit switches, etc.).

medium access control: The method of determining which data station has access to the network.

Copyright © 1991 IEEE All Rights Reserved

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS Not for Resale

message: The plant control information contained in a protocol data unit (PDU).

microcontrollers: A processing device that has the capability needed to receive data from external devices, analog or digital or both, process the data according to preset algorithms or special computing techniques or both, and then provide the results to external devices for the end purpose of controlling the process.

modulating control: Varying equipment as loads change. For example, modulating control may be used to vary the position of a control valve to maintain the liquid level of a tank. (Modulating control is sometimes referred to as regulating control.)

monitoring: A means of providing automatic performance supervision and alarming of the status of the process to the personnel and control programs, which may change the dynamics of the process.

multiprocessing: A computer organization mode of operation on a local basis in which multiple processors are working concurrently for high availability or high computing power or both.

motor control: A form of control that regulates the starting, running, and stopping of motors used to power operating equipment.

network management: A centralized or distributed network supervising service, complemented by a local service pertaining to each station (e.g., self-diagnosis), that monitors automatically the activity of all participants to the network linkage, diagnoses malfunctions, and recovers regular network service via reconfigurations, such as transfer to backup or standby services or equipment.

node: A device whose purpose is to provide communication through the main control network for one data station, a cluster of data stations, or a sub-network.

optical fiber: Any filament or fiber, made of dielectric materials, that guides light, whether or not it is used to transmit signals.

optimization: A function whose goal is to provide safe operation, minimize equipment wear, and to maximize efficiency.

outage time (OT): The accumulation of mean time to detection (MTTD) and mean time to repair (MTTR) during which the control system is not available to perform its function.

packet: The protocol data unit (PDU) that is used in a wide area network (WAN) with intermediate nodes between source and destination.

pitch: In a color CRT, the hole spacing in shadow masks that assures that each of the three electron beams (R,G,B) strikes only phosphor dots of the correspondent color.

pixel: Short for “picture element.” An addressable point (x, y coordinates) on a display screen.

plant: The totality of equipment that directly or indirectly converts a source of energy into electricity.

pre-failure state: The state of the system that, in the absence of any corrective action by the system, could lead to a failure.

process: The implied physics, chemistry, and energetic dynamics that take place during the conversion from a source of energy to electricity.

productive (active, intrinsic) redundancy: The kind of redundancy in which the redundant modules are used constantly for a background but productive task and undertake the task of a faulted module when this latter task is more important.

protocol: A strict procedure required to initiate and maintain communication.

protocol data unit (PDU): A frame, a protocol format, that is a complete sequence of binary symbols eventually completed with other non-data symbols, that is transmitted by a node and is received and understood correctly by the addressed node(s).

reliability: The characteristic of an item or system expressed by the probability that it will perform a required mission under stated conditions for a stated mission time.

 Copyright © 1991 IEEE All Rights Reserved

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS Not for Resale

replicated processing: The operation mode of multiprocessing in which several processors work the same program with the same data for fault tolerant purposes only.

reporting: The preparation of data to be further processed by the I/O of the system for man/process and man/machine interface.

response time of a distributed control system: The elapsed time between the moment when a signal is originated in an input device until the moment the corresponding processed signal is made available to the output device(s), assuming the input/output devices are located in the worst communication situation possible.

ring: A topology in which the nodes are linked through point-to-point communication in a closed loop.

routine broadcast: A network's service type that makes it possible for each participant to the network linkage to send messages cyclically, identified by a label, without destination; messages that may be received by a variable number of interested recipients in each cycle.

segregated system: A system that divides the hardware into subsystems along functional or technological lines.

self-diagnostics: An internal program, within a module, capable of locating faults.

semantics: The meaning associated with an object or its representation.

sequential control: A mode of control in which the control actions are executed consecutively.

spot size: The smallest area of light that can be produced by a CRT.

state of the art: The more advanced solution, already experienced with good results, offered by new technology to a given problem, but still applied by a few users. Eventually, the current state of the art will become the future common practice, and a new state of the art will replace the old.

sub-network: Serial network connecting data stations or communicating modules.

surveillance and disturbance analysis: A computer program that follows in depth the change of all process variables and determines the real causes of local or plantwide disturbances, sometimes issuing automated remedies or guidance to operators. It may or may not be based on expert systems.

system: The assemblage of hardware components and software modules structured and engineered to assure the performance of specified services.

system global time: The time elapsed between the moment an external event triggers a system reaction and the moment the system actuates a processed response.

three-dimensional (3-D): Stereoscopic images produced by more advanced video monitors superimposing a liquid crystal shutter over a CRT screen. With conventional color CRT, 3-D illusive images are obtained by using color encoded shades that give the impression of depth and volume.

tree: A topology derived from the bus, by branching the bus through active or passive splatters.

triad: In a color CRT, one set of red, green and blue phosphors.

unavailability: The ratio between the outage time and total of outage time and the time in which the system performs its duty. The unavailability figure is a value between 0 and 1, and equals (1 - A) where A = availability.

validation: The process of checking the correctness of a message, program or results.

verification: The act of confirming a message or a program correctness.

warm start-up: The procedure by which the system automatically undertakes, with the replacing piece, the functions of the replaced piece.

Copyright © 1991 IEEE All Rights Reserved

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS Not for Resale

3. Objectives of Distributed Control and Monitoring Systems

3.1 Introduction

The objectives of a distributed control and monitoring system for either a new plant or a retrofit include the following:

1) Greater dependability.
2) High plant efficiencies.
3) Improved response time to load changes.
4) Extended plant equipment life.
5) Improved operation.
6) Improved operator interface to the plant.
7) Improved accessibility of plant data.

3.2 Dependability

A system has dependability when reliability, availability and quality are integrated into the system design.

Availability as defined and used in this guide is a measure of the ratio of the time when a system is able to perform its duty and the total of this time and the outage time. Using this definition, various distributed control and monitoring systems can be evaluated for fault tolerance and dependability.

Distributed control and monitoring systems permit detection of a fault within the system using self-diagnostics. Because this detection is available, overall system reliability can be increased. When a fault occurred in non-digital systems, it was generally undetected until it caused a process upset. At this point operator intervention was generally required. On protection systems it was nearly impossible to detect the fault without activating the systems. Self-diagnostics provide two enhancements over previous systems, the first is increased unit safety and the second is increased control and monitoring system reliability. Unit safety is increased because upon fault detection, appropriate action can be initiated. This action can range from failure to a safe condition, to transfer to a back-up system where it is possible to maintain complete system functionality. Self-diagnostics also permits alerting operating personnel so that corrective action can be implemented. Since the mean time to detect (MTTD) a fault is reduced, which reduces the overall mean time to repair (MTTR), reliability of the system is increased. Modern fault tolerance techniques, which are offered in distributed control and monitoring systems include: hot repair, partitioning, and distributed redundancy. Section 8 of this guide provides a more detailed review of dependability.

3.3 Plant Efficiency

High plant efficiency during all modes of operation requires that equipment and process adjustments are optimized. This optimization minimizes wasted energy and heat rate during adjustments to transient conditions. A distributed control and monitoring system supports this goal by the flexibility of hardware and software configuration. Flexibility refers to the ability to change function, such as a control strategy, rapidly and easily. Flexibility is present because each function of a control strategy is implemented in software as opposed to hardware, as in pneumatic or electronic systems.

Flexibility is important during start-up of new plants to correct control problems. If, for example, it is determined that a feedforward is required, it can be implemented by changing the program. The new program can be developed and tested (eventually on a plant simulator) and then “downloaded” at a convenient time. With earlier systems, components may have had to have been procured, then when the unit was shut down, the hardware would be mounted and connected to the system—therefore, the time required to revise control strategy problems during start-up/testing was much longer.

 Copyright © 1991 IEEE All Rights Reserved

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS Not for Resale

During the life of a plant, control strategy changes may be required for several reasons. First, new control concepts that can improve plant performance will become available. Second, major components of the system may change, introducing new pulverizers, air heaters, etc. Third, plant operation may change, such as from base-loaded to cycling duty. With hardware-oriented systems it is difficult to modify or change the control concept, as any major change involves significant manpower and time to implement. With software-oriented systems, such as digital systems, the changes can often be accomplished without additional hardware, with little implementation time required.

Because software systems are easy to change, there is an incentive to take advantage of this feature and try different programs. If a change doesn't provide an improvement, it is easy to revert back to the previous strategy. Further, as experience is gained, additional parameters such as interlocks or calculations can be added to improve safety, effectiveness, and efficiency.

3.4 Improved Response Time

A power station is a highly interactive process, therefore, effecting greater integration of the various process loops will enhance overall system operation. While these interactions are readily accommodated by analog hardware, minor improvements in the mathematical model of the process becomes impractical sooner with analog than with distributed control and monitoring systems. As an example, faster control response to process changes can be obtained by adding feedforward between mildly interactive loops, which was impractical with analog systems (i.e., unit load control and feedwater heater level control).

The data communication network is a critical component in determining response time. Therefore, Sections 5 and 6 of this guide address this topic.

3.5 Extended Equipment Life

Automation reduces the number of human errors during both normal and emergency situations because appropriate responses are preprogrammed into the database. As an example, the system starts up and shuts down plant equipment with a minimum of operator errors, thereby extending the equipment life. Automation can provide control of temperature ramping to protect mechanical equipment from thermally induced stress cycle failures, a procedure that would otherwise require manual control with conventional control systems.

3.6 Improved Operation

Distributed control and monitoring systems lend themselves to better process supervision and automation. Calculations and nonlinear functions such as square root, thermocouple conversion, and nonlinear control are easily performed using a symbolic control language. Such features as adaptive control and self-tuning of control constants, along with advanced control algorithms, such as those that provide predictive control actions, can be relatively easily implemented within distributed control and monitoring systems. Artificial intelligence and statistical process control are other advancements that will increase the benefit of distributed control and monitoring systems.

3.7 Improved Operator Interface

Distributed control and monitoring systems feature a better display and operating facility structure, based on cathode ray tubes (CRTs). The improvement over indicators, recorders, and alarm panels on panel boards is that data and images can be presented to the operator. The key word here is "presented"—raw data doesn't just have to be displayed, but rather, information and guidance is provided to the operator in a usable format. Alarms can indicate a situation requiring operator interaction, and not just display status. Guidance can be provided and effects of control actions can be analyzed before being implemented. The effects of better information display and increased automation can serve to improve the plant's efficient and dependable operation and allows the operator to supervise the control system rather than having to be an integral part of the system.

Copyright © 1991 IEEE All Rights Reserved

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS Not for Resale

Distributed control and monitoring systems provide the capability for communications between devices over a common circuit, or at least a minimum number of circuits. These circuits are called data communication networks. Control loops connected through these networks can receive plant data concurrently and utilize the data in their control loop. The prime result is increased automation and an improved man/machine interface. Man/machine interfaces are discussed in greater detail in Section 7 of this document.

3.8 Accessibility of Plant Data

The distributed control and monitoring system will contain plant data that may be accessed and utilized for many diverse activities. This data can be used by both engineering and management personnel. Some of the engineering uses include: optimization of control strategies and development of alternative control modes. Proposed changes can be developed and evaluated prior to implementation. It must be stressed that any usage of data is dependent upon the consistency of the data with other data being considered. This information consistency and time validity is addressed in Section 5. Management use of plant data will allow monitoring of plant performance and efficiency. It will also permit a continuous review of equipment status and performance to be used for outage planning.

Distributed systems provide data throughout the network; therefore, plant data can be made available at multiple locations throughout the plant instead of a concentration in the control room area. This means that data stations (human interfaces) may be located in the maintenance shop, instrument calibration room, chemical lab and administration offices. The man-machine interfaces and data acquisition are further described in Section 7.

3.9 Cost-Related Factors

Distributed control and monitoring systems can be economically attractive in three areas: initial investment, installation, and intangibles. Distributed control and monitoring systems often cost less than an equal analog system or a central plant computer due to such factors as equipment/parts availability, modular programming vs. application programs with many subroutines, and the need for a smaller quantity of spare parts. Installation of distributed control and monitoring systems may offer savings, especially in new plants. Less space is required for both the electrical room and the control room. Furthermore, little or no panel is required since the operator interface is through CRTs. When data has to be collected from distant locations in the plant, and the system is geographically located, data can be transmitted over the data communication network, offering a significant savings on cable and installation. Additionally, distributed control and monitoring systems lend themselves to automation that provides intangible savings, such as assuring that the same equipment operating procedures are followed, regardless of the operator, thereby minimizing stress and prolonging the life of the equipment.

Digital technology has made functions that were economically unattractive into standard features. A new feature available with distributed control and monitoring systems is its drift-free calibration and tuning. Another potential improvement is the use of a “field bus,” which has the possibility of reducing system cost and improving reliability by eliminating the dual conversions of D/A and A/D. In most cases, the capabilities attributed to digital systems have always been available. Fault detection, for example, has been available with analog systems: a comparison is made between three identical data sets, and if one set deviated from the other two sets, it was assumed to have a fault. The cost of such an approach exceeds the base digital system by at least a factor of three. Because of the economics involved, this approach is seldom used.

4. System Application Issues

4.1 Introduction

This section of the Guide is concerned with application issues that arise in applying distributed digital systems to a power plant. The following topics are addressed:

Copyright © 1991 IEEE All Rights Reserved

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS Not for Resale

1) Integrated vs. Segregated Systems
2) Functional and Geographic Distribution
3) Hierarchical Architecture and Automation
4) Control and Protection Functions
5) Input/Output System
6) Environmental Considerations
7) Documentation

4.1.1 Control Philosophy

A comprehensive and well-defined control philosophy should be established at the outset of any project, whether a new generating station, or a retrofit of a portion of an existing plant control system. Control philosophy is the totality of concepts on which the power plant control system is based. It evolves from consideration of the specific plant requirements, experience on other, similar, plants, and assessment of the technology available at the time the system is to be implemented. It includes consideration of the types and degree of control and monitoring tasks to be provided, specific features to be provided, and the approaches to be taken to the various application issues discussed in this section. Wherever possible, objective criteria should be established to enable all parties in the application of the distributed control and monitoring system to have a clear understanding of the goals of the project.

4.1.2 Specifications

Prior to issuing specifications interface requirements among the owner, the operator, the engineer, the manufacturer of the distributed control and monitoring system, and other equipment manufacturers or suppliers should be established to facilitate and expedite the complex engineering the system requires. These tasks include:

1) Definition of the division of responsibilities among the parties involved in the application of the system.
2) Preparation of a detailed specification for the distributed system manufacturer, defining his scope of supply and responsibilities.
3) Establishing administrative procedures and communication guidelines among the parties involved in the application.
4) Preparation of detailed specifications for equipment defining the signal interface required between the distributed system manufacturer, and other equipment manufacturers.

4.1.2.1 Changes

Specifications for the distributed digital control and monitoring system will normally evolve with the design of the plant, and therefore should incorporate provisions for modifications.

4.1.2.2 Operator Interface

The operator interface should be consistent for all control and monitoring functions in order to achieve an integrated human interface consistent with the principles of human engineering (see Section 7, Data Acquisition and Monitoring). A uniform set of CRT display and control panel design-conventions should be provided for the total system. Each CRT display should be capable of both control and monitoring as required.

4.1.2.3 Vendors

Vendors of major equipment should be required to conform to plant instrumentation and control standards to prevent a multiplicity of systems. This requires early project definition of the instrumentation system requirements.

4.1.2.4 Dependability

A dependability analysis should be considered when specifying a distributed control system (see Section 8, Reliability, Availability, and Fault Tolerance of Distributed Control and Monitoring Systems). In general, the system should be

Copyright © 1991 IEEE All Rights Reserved

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS Not for Resale

designed and configured such that failures are localized to the extent that no single failure causes loss of monitoring or control over more than an isolatable minimum portion of the plant.

4.2 Integrated vs. Segregated Systems

4.2.1 Scope

When a digital control system is to be installed in a plant, either as a retrofit at an existing plant or as an element of a new generating station, the first consideration is to establish the system's scope. A major factor in this determination is the degree to which control and monitoring functions are to be integrated into a common system. A range of alternate configurations, from fully integrated to completely segregated, can be established. Complete integration of the plant control system components will yield several advantages as described throughout this Application Guide.

4.2.2 Integrated Systems

A fully integrated system consists of common hardware and software structures, and a common data communication structure, assembled to form a uniform plant-wide control system with global access to all data therein. An integrated system permits a full range of control and monitoring functions, including discrete and modulating control, sequential control, supervisory control, and techniques such as expert systems and statistical process control to be performed within the context of these common structures. This generally requires that the entire system be supplied by a single control system manufacturer, although adoption and successful demonstration of an industry standard communications structure suitable for power plant control would make this unnecessary. An integrated system may be divided into subsystems along functional lines, but these subsystems are essentially transparent to the control and monitoring tasks, and in no way impede the flow of data through the system. A form of "quasi-integration" can be obtained by merging diverse digital systems or networks through gateways or by cross-wiring between the I/O structures of diverse systems.

4.2.3 Segregated Systems

A segregated system is comprised of several independent control systems, based on a concentration of similar functions such as binary vs. modulating control, monitoring vs. control tasks, or based on a narrow scope of the plant control task, without a common hardware and software structure, and without a common data communications structure. Historically, power plant control systems have used segregated control and monitoring systems because of the nature of the available hardware. Binary control was by electromechanical relays, modulating control by electronic analog equipment, and monitoring by a mainframe computer. Segregation has been further enforced by the practice of engineering and purchasing control systems with major mechanical components and subsystems. Subsystems such as demineralizers and ash and coal handling systems, which consist almost entirely of binary logic, have evolved to use independent programmable controllers that are suited to this task. Likewise specialized digital hardware has been developed for other mechanical components from the air compressors to the turbine generator. Some degree of segregation is almost assured in modernizing an existing plant, because it is generally impractical to replace subsystems that are operating properly to gain the additional advantages of an integrated system.

4.2.4 Advantages of Integrated Systems

The major advantage of a fully integrated system is the universal availability of all data. This permits data used in a control or monitoring task to be used in other tasks as well, thereby improving the model of the plant processes available to the operator, improving the control and monitoring schemes in the system, and allowing the optimization of software for control of the entire power plant as a single process. Advantages of a fully integrated system are as follows:

1) All data is universally available for control, monitoring (including alarms), operator displays, data acquisition, performance monitoring, and other functions. Moreover, features such as the ability to modify programs in any portion of the system, to upload and download programs, etc., are inherent in the system.

Copyright © 1991 IEEE All Rights Reserved

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS Not for Resale

2) Hardware types are minimized, greatly reducing spare parts inventories, training requirements, troubleshooting and maintenance procedures.
3) Software structures are uniform throughout the system, again minimizing training requirements and permitting the use of common control and monitoring schemes throughout the plant.
4) Gateways are eliminated, eliminating the associated hardware and software. (It should be noted that a gateway introduces a delay and a potential point of failure into the system. Refer to Sections 5, 6, and 8)
5) If desired, the system manufacturer can be established as a single point of responsibility for the entire control and monitoring system. This, of course, requires that the manufacturer maintains a staff with well-established experience in all aspects of power plant control.
6) Benefits not economical in segregated systems, such as the ability to trend any data point, can be provided at little or no incremental cost.

4.2.5 Disadvantages of Integrated Systems

Disadvantages of an integrated system include the following:

1) The control and monitoring tasks of a large generating station could potentially exceed the capacity of some systems. When implementing a digital system, careful attention should be paid to the capacity not only to perform the specified task, but also for future expansion, in terms of both hardware and software. It should be noted that an absolute maximum capacity exists for many parameters of the system, a case that did not exist with analog control systems.
2) Selection of a commercially available distributed control system will require trade-offs among the various features offered by each of these systems. Use of a single system throughout the plant requires that the features offered by such a system be sufficient for all of the control and monitoring tasks contemplated.
3) A design defect in one portion of the system may be duplicated throughout the integrated system, and could therefore take significant time to correct.
4) Application of a fully integrated control system will generally require more comprehensive front-end engineering than will a comparable segregated system.

4.2.6 Advantages of Segregated Systems

Advantages of a segregated system are as follows:

1) Control systems may be purchased with the associated mechanical hardware package, taking advantage of pre-engineered control schemes. Typical examples of such packages include polishers and demineralizers, ash handling, coal handling, precipitator or baghouse, soot-blowers, etc.
2) Responsibility for control of various portions of the plant can be placed with the party most familiar with the control of that equipment or process; for example, manufacturers are generally the most familiar with their product. This approach can also be taken with an integrated system, but it requires a significantly greater coordination effort.
3) The type of control equipment used can be matched more closely to the process or equipment under control. This concept applies particularly to the application of specialized equipment for processes such as precipitator field voltage control.

4.2.7 Disadvantages of Segregated Systems

Disadvantages of a segregated system include the following:

1) Data is not available throughout the plant without special efforts. Therefore, if data from a control island, such as the demineralizer, is needed for control or for a monitoring or optimization routine, this data must be accessed through a gateway or hardwired between I/O structures to make it available to the external system.
2) A non-uniform operator interface consisting of multiple independent devices is typically encountered, or extra efforts are required to establish a consistent operator interface.
3) Coordination or duplication of functions across system boundaries is difficult.

Copyright © 1991 IEEE All Rights Reserved

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS Not for Resale

4) Greater quantities of spare parts and training are required.

4.2.8 Guidelines for Degree of Integration

As mentioned above, although a fully integrated plant control and monitoring system is possible, has many advantages, and should be encouraged, it is likely that the best application for most plants will lie between the two extremes. The following guidelines should be considered in establishing the degree of integration:

1) Where the control tasks to be performed require interaction between subsystems, serious consideration should be given to integrating these subsystems to ensure timely, reliable exchange of data between subsystems.
2) Where subsystems are to be controlled through a common operator interface, or are to be included in a common monitoring system, consideration should be given to integrating these subsystems.
3) Where significant collection of data is required for data acquisition and logging, performance monitoring, diagnostic maintenance programs, etc., consideration should be given to integrating the subsystems to be monitored.
4) Within an integrated system, data networks can be established with sufficient security and speed of response to be acceptable for real time control. The use of gateways for real-time control should be discouraged for dependability and timing considerations, although for time decoupled tasks they may be acceptable. (Refer to Sections 5, 6, and 8 for further information on this topic.)
5) The capacity limitations of the candidate systems being considered should be kept in mind as functions and I/O are added to the integrated system. A margin should be maintained in all limited system resources, such as memory, response time, point count, etc., to permit future modifications to the system.
6) Where a segregated approach is to be followed, the number of different system manufacturers and unique hardware designs should be minimized in consideration of training, spare parts, and the capability for future networking. Avoid the use of prototype or one-of-a-kind designs to the extent possible.
7) Certain protective functions should have a minimum of interposing logic devices, and should be directly hardwired from the initiating to the actuating device. An example of such a function is control over the dc lube oil pump.

4.3 Functional and Geographic Distribution

In common practice, functional and geographic distribution are two principles followed in choosing the location of hardware modules and assigning tasks to the data stations of the distributed system. These terms refer to the perspective from which the user views the system as application programs are implemented. In functional distribution, the accent is on maintaining the integrity of each function within an individual data station. With geographic distribution, functionality is assumed a given, and the system is deployed in accordance with the physical layout of the plant, minimum wiring criterion, and specific environmental local requirements. Although these distributions can conflict with one another, they also complement each other when judiciously applied. These two approaches should therefore be viewed as complementary rather than opposites. Application of these principles may have important consequences on plant operation, repair, maintenance, and future extensions to the system.

Although the earliest pneumatic and electromechanical controls could be considered both functionally and geographically distributed, this guide is limited to digital applications. Regardless of whether data processing units are located in a centralized room, sited remotely in an environmentally controlled area, or mounted in the field at the process area, all loop information, access to set points, and manual control are required in the control room (see Section 7).

With the advent of the field bus, the generalized use of microtechnology for remote control, and more secure and faster networks, the functional distribution concept has been generalized to refer to tasks executed in sets or clusters of stations linked through field buses, subnetworks, and superimposed networks. The goal of this distribution is to implement an automation hierarchy of local, group, and unit controls (see 4.4), while incorporating fault tolerance, optimization, and other advanced techniques. Such a distribution favors the use of multivariable transmitters and

 Copyright © 1991 IEEE All Rights Reserved

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS Not for Resale

multivariable controllers, and represents the state of the art. The definition of functional distribution is therefore evolving with the technology to refer to a distribution of programs among distinct hardware capacities partitioned according to control and hierarchical tasks.

However, such a definition tends to blur the distinction between functional and geographical distribution.

For a better understanding and for its continuous use in some small environments, the following subsections refer to the common practice definition as mentioned above.

4.3.1 Functional Distribution

In general, the term functional distribution refers to the practice of implementing an entire applications task or group of related tasks within a given station, without the need for the support of any other stations on the network. In practice, the term has come to refer to the strategy of implementing a control loop entirely within a single station, such that neither the process data nor the control signal output to the actuator is passed through the data communications network. (Operator intervention through CRT commands, is of course through the network.)

4.3.1.1 Advantages of Functional Distribution

Advantages of functional distribution of the application tasks to be performed in the distributed system include:

1) Control response time is not dependent upon the data communication system response time between data stations, because the network is not used for control signal paths. It should be noted, however, that the response time of data communications within the data station is a component of the control response time.
2) The control task is independent of the data communications task, and can therefore remain operational in the event of failures in the communication system.
3) The effects of loss of a single data station can be isolated to a particular functional group or task within the power plant, such as to a single pulverizer.
4) The task of configuring an individual data station is somewhat simplified because all required data is resident in that station. (This advantage is moot in systems where the location of individual data points is transparent to the user.)

4.3.1.2 Disadvantages of Functional Distribution

Disadvantages of functional distribution include:

1) Field wiring costs may increase in installations where the system is both functionally and geographically distributed, because functionally related instruments and drives are not necessarily confined to a small area of the plant.
2) The inherent advantage of the universal availability of data in the system is compromised to the extent that use of the data communications network for control purposes is avoided.
3) The task of assigning I/O wiring to the system cabinets becomes dependent upon the station in which the control is to be accomplished, requiring that these be sequential rather than independent efforts, which can have significant impact on design and procurement schedules.

4.3.2 Geographical Distribution

Geographical distribution positions data stations near the field equipment, irrespective of process functions. Thus, the input for a control circuit and the output to the associated actuator may be in different stations, linked together by the data communications network. Therefore, a prerequisite for geographical distribution is a secure, high-speed, intraplant data network; secure because loss of communications is loss of control, and high-speed because otherwise response times between a value-change and the reaction of the actuator might be too long.

Copyright © 1991 IEEE All Rights Reserved

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS Not for Resale

4.3.2.1 Advantages of Geographical Distribution

Advantages of geographical distribution include the following:

1) A potential savings in I/O wiring costs, particularly if data stations can be located near concentrations of I/O. This savings multiplies when consequential costs for raceway and building volume are considered.
2) Reduction of cable concentration associated with geographical distribution reduces the fire hazard as well.
3) A degree of fault containment against environmental disasters such as fire, can be obtained. (Although, if other stations functions' depend on data from the damaged station, this advantage diminishes and can in fact become a disadvantage.)
4) The number of I/O points per station can frequently be reduced, leading to additional reliability through fault isolation, although at the cost of more stations for a given I/O count.
5) Retrofits of additional circuits to the system can be accomplished at significantly reduced cost, provided sufficient expansion capacity has been designed into the original system.

4.3.2.2 Disadvantages of Geographical Distribution

Disadvantages of geographical distribution include:

1) There is a small, yet finite increase in control response time and some decrease in dependability associated with the use of the data network as a path in the control circuit.
2) Failure of a single station can have widespread effects on plant operations.
3) There is a potential for an increase in the amount of hardware required for the system.

4.3.3 Distribution Suggestions

Functional and geographical distribution are not mutually exclusive. Elements of both will be present in most practical systems. The following recommendations should help in selecting the appropriate philosophy for a given plant:

1) Where concentrations of field devices can be identified in the plant, geographical distribution of the system will yield an economic advantage, especially using field buses. Prerequisites for this arrangement, however, are suitability of the hardware for the proposed environment, and proper speed and security of the data communications network. Criteria for the network are given in Section 5, Data Communications Structure.
2) Care should be taken to avoid exposure of the data network to environmental hazards. Environmental criteria are discussed in 4.6.
3) Where extreme speed of response is essential, or where data communications are not sufficiently secure, functional distribution should be applied.
4) When functional distribution is applied, care should be exercised to ensure that failure of a single station has minimal effect on plant operation: i.e., that, to the greatest extent possible, a single data station serves process segments that are interdependent.
5) Highly interactive control systems, such as combustion controls, can exceed the capacity of a single data station. Where this occurs, consideration should be given to the method of distribution to be used to effect the implementation of the control system. Both functional and geographic distribution can be established by dedicating an individual station to process segments such as individual pulverizers. The dependability and speed of the data communications network will determine whether the demand signals to the individual pulverizers are hardwired or transmitted through the network. Guidance on these issues is given in Sections 5 and 8
6) The application engineer should be aware that although the system hardware is distributed, either functionally or geographically, the system software remains an integrated whole through the data communications network. While distribution of hardware can isolate many types of hardware faults, software faults, without proper containment, can cause failures in otherwise independent stations.

Copyright © 1991 IEEE All Rights Reserved

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS Not for Resale

4.3.3.1 Evolution Considerations

As microtechnology continues to permeate the instrumentation and control industry, data communication through multilevel networks may effectively mask the physical connotations of functional distribution as the data communication networks come to be considered a universal “software bus”—a utility which provides data transfer services, much as the plant air headers provide motive power. Even in such an advanced system, however, the principles of functional and geographical distribution, as discussed in 4.3, should be considered in the allocation of control and monitoring tasks to data stations, networks, and subnetworks. Implementation of functional distribution of software coding with geographical distribution of the system hardware to match control equipment with mechanical equipment should be considered, and optimization of such distribution, in order to establish the highest dependability, availability, functionality, fastest response time, and lowest cost should be the application engineer’s goal. These objectives are further served through the application of the principles of hierarchical software and hardware structures discussed in the following section.

4.4 Hierarchical Architecture and Automation

The decision to utilize a distributed control and monitoring system for overall power plant control offers an opportunity for a high degree of automation. Automating the power plant is expected to increase overall plant availability, efficiency, and operational safety. A hierarchical structure is a form of functional distribution that can facilitate automation (see Section 6).

4.4.1 Hierarchical Structure

While the hardware is distributed, the software should be thought of as a continuous, uninterrupted sphere of the plant intelligence, working in a structured, hierarchical way, as one well-organized entity. Hierarchical organization of software provides coordination of tasks, organized supervision, manual intervention at appropriate levels, and is well suited to the implementation of fault tolerant techniques.

4.4.1.1 Software Structures

The hierarchical structure of control and monitoring functions does not necessarily require a similar hierarchical distribution of the data network and its data stations. That is, software structures can be arranged in a hierarchical manner within individual data stations.

4.4.1.2 Control Functions

Control functions are usually hierarchically structured on several levels: the local or drive level, the group level, and the plant unit level. At each level increased intelligence regarding the status of the process is obtained and raw data can be reduced to information more readily useful to the operator.

4.4.1.3 Functional Levels

Several tiers of functional group levels can be established between the individual drives and the highest or plant control level as required for the particular plant process under control. For example, more levels would be required for the feedwater system than would be required for the precipitator.

4.4.1.4 Functionality

The design of the hierarchical automation structure should include the following features:

1) The system should be functionally subdivided into recognizable modular subsystems that operators and maintenance personnel can easily identify.

Copyright © 1991 IEEE All Rights Reserved

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS Not for Resale

2) A malfunction or failure should only affect a specific piece of equipment or a very limited portion of the system.
3) If the system cannot operate at the higher levels, the lower levels should be capable of independent operation.

4.4.1.5 Hierarchical Structure

Figure 2 illustrates hierarchical structure and shows the various levels.

4.4.1.5.1 Drive Level

The lowest level of the structure is the drive control. A drive is, for example, motor operated equipment (pump, fan, valve, damper), solenoid operated equipment (valve, damper), or a modulating drive (valve positioner, variable frequency drive). At this level, each drive can be started or positioned manually or automatically and has its own interlocks and protection programmed in the distributed control system to insure independent safe operation at this level.

It is also at this level that alarms receive the first level of processing above that performed on the input card. Here, signals can be compared with other concurrent data and reasonability checks expanded to make use of the additional information available.

4.4.1.5.2 Group Level

Functional group control is the next level in the hierarchy. Here, drives are grouped functionally; for example, a pump set and related valves would constitute a group. Some measurements may also be routed directly to the group level as appropriate. Manual/automatic capability may be provided at this level. The independent capability of drive level segments is maintained when these controls are placed under the supervision of a group controller. This capability permits the coordination of each process segment in each operational mode of the plant, such as start-up, steady state, cycling, and safe shutdown for routine or emergency cases.

At the group level, verification and cross validation of measurements, including consideration of validity time, prioritization of alarming signals, reduction to the prime alarming signals and other distributed higher level programs such as optimization, preventive alarming, expert system and process simulation can be initiated or expanded upon. Even though, for alarming purposes, the alarm signals are reduced to the prime ones, all measured values and events should be reported to the monitoring function at the unit level (see Section 7).

4.4.1.5.3 Unit Level

The highest level of the hierarchy is the unit control. This level combines and coordinates the functional groups to operate as a unit and expands upon the processing done at the group level. Obviously, this principle can be extended to coordinate the operation of several units (plant level), or several plants (system level). At the unit level, all group controls are dynamically balanced and supervised. Additional functions performed at the unit level are discussed in Section 7

4.4.2 Automation

Plant automation requires that the plant equipment be brought into a desired operating mode and optimized in that operating mode, that upsets be prevented, and that shutdown be initiated, if necessary—all with little, if any, manual intervention.

Copyright © 1991 IEEE All Rights Reserved

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS Not for Resale

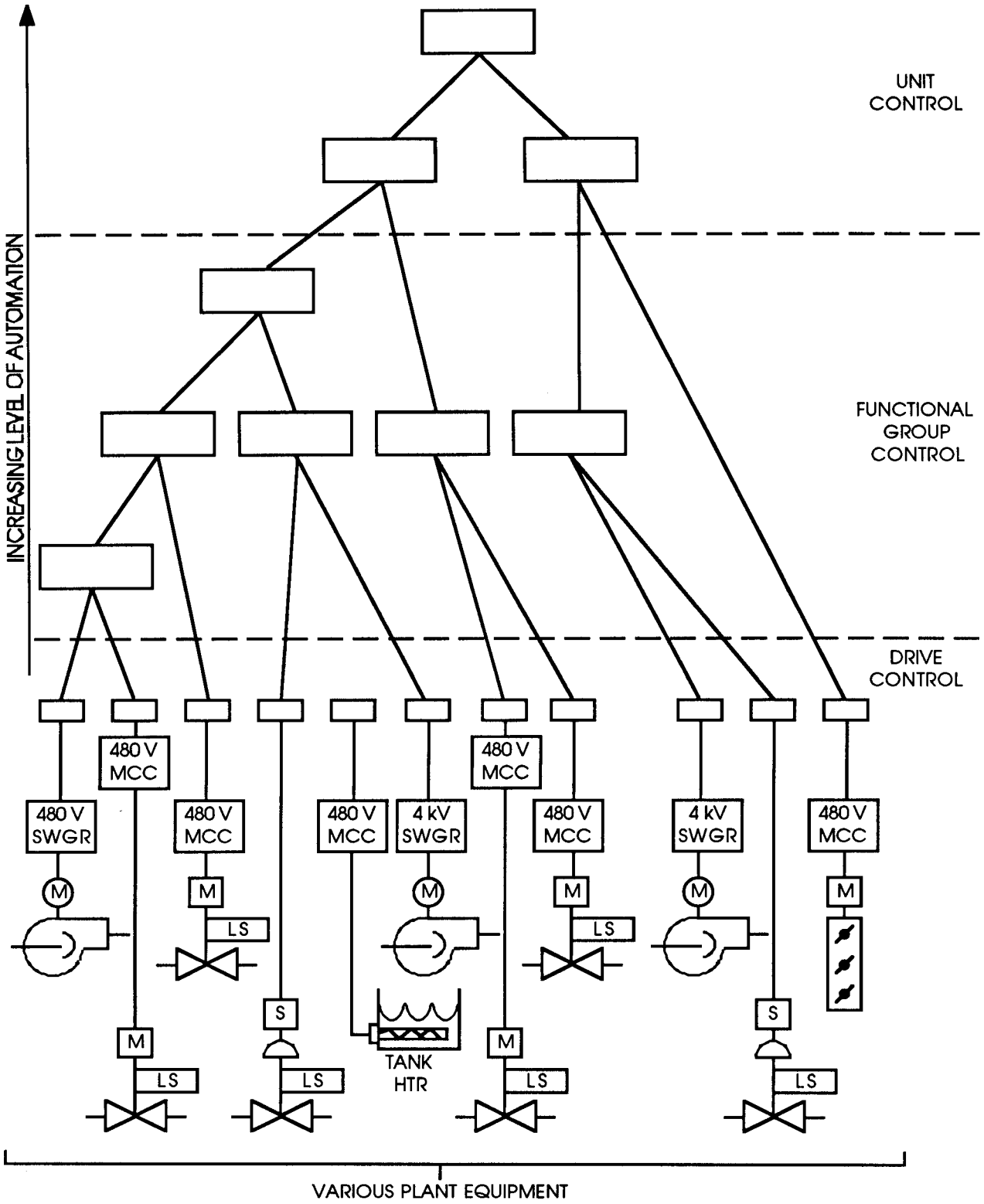


Figure 2—Hierarchical Structure

Copyright © 1991 IEEE All Rights Reserved

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS
Not for Resale

4.4.2.1 Coordinated Operation

Automation requires coordinated operation of multiple devices, which can most logically be performed through a hierarchical control structure; hence, establishing a hierarchical automation structure becomes the most important concept in any automation system (see Fig 2). Hierarchical organization and automation share many common features.

4.4.2.2 Operational Modes Transitions

An important objective of automation is the orderly and quick transition from one operational mode to another, such as start-up, load changes, run-backs, and shut-down. Coordination of plant equipment during the change from one mode to another is accomplished by a sequence of commands given by the unit level to the group level, and by the group level to the local controls. Each level maintains supervision over equipment and process status, adjusting them as required to move to the new state.

4.4.2.3 Manual Intervention

If an external event, or process disturbance, occurs and cannot be accommodated by the predefined control strategy, manual intervention may be necessary to permit the automated transition to the next step in the sequence. (e.g., the operator may be permitted to override a failed limit switch, once properly identified, to continue the automatic sequence.)

4.4.2.4 CRT Information

CRT displays of control sequence diagrams, charts, or mimic diagrams identifying criteria for state changes, status of each criterion (fulfilled or non-fulfilled), current activity, and any other useful information should be available to the operator. During manual operation these diagrams should specify the required operator actions.

4.4.2.5 Advantages of Automation

The most important advantages that can be realized by implementing a high level of automation are the reduction of operator decisions and errors during emergencies, and extending equipment life by starting and stopping the plant equipment the same way each and every time. Automation can enforce a reduction in the number of large motor starts per hour, automatically select redundant equipment to ensure equal wear, and in conjunction with process systems such as turbine bypass, can provide substantial fuel savings because it allows faster run-up time and lower run-up losses.

4.4.2.6 Advanced Features

Features such as statistical process control and expert systems can be expected to develop to the point where they further improve the ability of the distributed system to keep the plant in an optimum operating state. These features may be implemented at various levels in the automation structure through a logically functional distribution.

4.4.2.7 Operator Skills

While increased automation reduces the burden on the plant operator, care should be taken to ensure that this does not isolate the operator from the plant process. Properly applied, the automation system should prevent improper actions, and should take immediate protective or regulating control action where sufficient data is available to fully define the correct control response. Where appropriate, the operator should be maintained as an integral part of the plant control scheme to ensure the required skills for manual control are kept sharp.

Copyright © 1991 IEEE All Rights Reserved

--`,,`,,`-`-`,,`,,`,`,,`---

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS Not for Resale

4.5 Control and Protection Functions

The primary purpose of a distributed digital control and monitoring system is to maintain control over the plant processes. While the system may be expected to perform various other tasks, this task should be the highest priority. (Automatic protective actions are considered control actions in this context.) This section does not deal with control strategies or how to perform specific control tasks. Rather, it discusses issues related to distributed control systems and their applications to power plants.

The issues of integration, distribution, and hierarchical structure discussed in the previous sections have a significant impact on the performance of a distributed control system and should be carefully considered as the system is selected and applied.

Binary logic is associated with nearly every actuated device in the power plant to assure safe and proper operation. Many of these same devices are also positioned by modulating controls, and sequenced for purposes of plant automation.

4.5.1 Control Tasks

Control tasks include both automatic operations to maintain desired operating conditions in the plant equipment and processes, and manual operations in which the operator makes these adjustments.

4.5.1.1 Increased Power

The increased power of microprocessor based control equipment permits the use of more extensive and adaptive control techniques, and optimized control schemes in which the competing objectives of maximum efficiency, lowest cost, longest equipment life, and minimum environmental effects (among others), may be dynamically balanced on a continuous basis.

4.5.1.2 New Techniques

Techniques rooted in artificial intelligence have led to such features as self-tuning controllers, in which controller tuning parameters (gains, integral action, etc.) are dynamically adjusted without operator intervention to maintain precise control over processes with time varying response criteria.

4.5.1.3 Considerations

Considerations that the applications engineer should take into account include the following:

1) The system should be readily configurable and capable of on-line reconfiguration and maintenance. It should be self-documenting, fault tolerant, highly dependable, and reliable.
2) The selected system should be provided with a set of predefined control algorithms capable of performing all of the control functions required for the plant. A library of these algorithms should be resident in the system's memories.
3) Control algorithms are not standardized across the industry, even to the extent that the PID (proportional + integral + derivative) equations used by various manufacturers differ significantly [B1] .[1] The engineer should be aware of these differences.
4) The engineer should consider the method provided to ensure the integrity of the control memories, including the control algorithm library. Various types of nonvolatile memories, and battery backed volatile memories are available. PROM is generally suggested for "standard" algorithms, with RAM considered for more extensive or specialized programming, and application-specific programming.

[1]Numbers in brackets correspond to numbers in the Bibliography in Section 9

Copyright © 1991 IEEE All Rights Reserved

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS Not for Resale

5) The data station should provide for timely execution of these algorithms. Where values are generated in different data stations and transmitted through the communication structure for use in control, care should be taken to assure that delays in receiving the data do not cause timing problems in the logic.
6) The response time of the control actions taken by the system should be sufficient to maintain control over the process under all operating scenarios. This response time should include consideration of delays and dead times, both internal and external to the digital control system, and should be selected based upon the process requirements. Section 5 deals with response times for the data communication networks of the distributed control and monitoring system. The response times discussed here include those times as well as processing times, I/O scans, etc. As improvements are made in process sensors and actuators, the controller response time, including data communication times, will become more significant.
The control system should transfer to manual control and alarm upon loss of valid process data. Where practical, a graceful degradation should be established by the application engineer.
The response times in Table 1 are for the distributed control system portion of the response time only, exclusive of sensor, impulse line, and actuator, and are provided as a general guideline. The particular requirements for any given application should be established by the application engineer as shown in Table 1. In evaluating these response times, the application engineer should consider worst-case network and system loading, taking into account such events as unit upsets or trips, configuration up or down loads, and controller failover.

Table 1—Distributed System Typical Response Times

Function	Response Time
“slow” loops (e.g., most temperatures)	250–1000 ms
“fast” loops (e.g., some pressures, flows)	50–250 ms
binary control	100 ms
protective logic	1–100 ms

7) The system should permit software access to all points in internal algorithms that may be useful in developing a control strategy for a particular plant. For example, the applications engineer may wish to change controller tuning parameters based upon an external determination of the plant status.
8) Conversely, the system should provide a means to limit access to parameters, such as protection related setpoints, that should not be modified except by authorized personnel. Because the degree of access to be provided to the operator will vary with the application, this should be a user-definable parameter, protected by password, key switch, removable key panel, or similar means.
   a) Engineered setpoints that do not require operator adjustment should be displayed, but not accessible to the operator.
   b) Controller tuning parameters should generally be accessible only to the plant engineer or instrument technician so as to avoid upsets to the process caused by unauthorized changes.
9) The system should be sufficiently dependable and reliable to ensure that the control system is not a significant source of unit downtime or reduced capacity.
10) The system should be configured such that controllers may remain in automatic control as long as valid process data is available. Input signals should be scaled such that valid data is provided to the control system even in upset conditions.

4.5.2 Protection Functions

Protective functions are almost always binary control functions, generally require very fast response times, and have little operator interface other than notification. Protective functions should be very dependable and designed to prevent either false trips, or failure to trip. Protective actions can be initiated based on an event, a threshold value, operator intervention, or an analysis of the plant status. Although many protective devices, such as motor overloads, are merged

Copyright © 1991 IEEE All Rights Reserved

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS Not for Resale

into normal control circuits, conventional practice has separated protective functions from normal control actions in sophisticated systems, such as furnace safety and turbine overspeed protection. The applicable safety codes governing each installation should be consulted for guidance in this area. Some jurisdictions may require that independent systems or dedicated data stations are used for protective functions.

4.5.2.1 Response Time Requirements

The response time requirements for protective functions may in some cases require that the entire function be performed in a single module of the distributed system, such that the function is served by a dedicated fault-tolerant microprocessor. An example of such a situation is turbine overspeed protection, in which the redundant speed sensors are monitored and compared to the trip point by a dedicated microprocessor that provides, within the same module, a trip output to the turbine stop valves. In such a system, data would be passed to other levels of the system for other functions such as speed/load control, monitoring, etc.

4.5.2.2 Protective Function Security

Transfer of data from protective functions to control and monitoring functions should not be made in such a way as to compromise the protective function. That is, failure or loss of an operating component should not cause a protective function to be disabled.

4.5.2.3 Testing

Protection functions require periodic testing and calibration separate from the requirements for testing and calibration for normal control equipment. The distributed system should recognize and accommodate this requirement.

4.5.2.4 Furnace Safety

Furnace safety and burner management systems should generally be assigned to dedicated stations, whether the plant controls are realized in a segregated or in an integrated system. System integrity and security considerations require a high degree of isolation from other control and logic systems and conformance to current boiler process parameters. These systems should always comply with the applicable NFPA 85 series standards.

4.5.2.5 Interlocking and Protection

Although interlocking and protection in hardwired form is still being installed in power generating stations, microprocessor-based logic has gained acceptance and has demonstrated a high degree of dependability. It should be recognized that fault-tolerant, microprocessor-based control systems, including elements of data networks, for safety-related applications in various plant subsystems, have been with us for some time now. The key to successful application is a very careful, conservative, and properly applied fault tolerant structure, and assurance that response time is adequate for each situation. With these attributes, a microprocessor-based system can exceed the dependability and availability characteristics of equivalent hardwired systems.

4.5.3 Configuration and Tuning

The control and monitoring system should have “friendly” functional and logic programming, such that the system is configured, rather than programmed. Symbology used in configuration should follow industry standards for graphical presentation of logic, such as IEEE, IEC, SAMA, ISA, or similar standards as appropriate to the project. Both binary logic diagrams, using ladder or other graphic logic language, and functional control diagrams, based on SAMA or equivalent symbols, should be provided in a graphical programming environment in which functions are linked as on a drawing.

Copyright © 1991 IEEE All Rights Reserved

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS Not for Resale

4.5.3.1 Program Languages

Other languages, particularly those that permit portability of software among computer systems, such as C, Pascal, Fortran, etc., should also be supported for advanced control programming.

4.5.3.2 Specialized Algorithms

The system should allow the application engineer to write specialized control algorithms as may be required for unique control problems in his plant. These algorithms should then be used in the same way, with the same facility, as the manufacturer's standard algorithms.

4.5.3.3 Standard Algorithms

In some cases, a user may wish to modify a standard algorithm as supplied by the system manufacturer. This practice should be discouraged. Where it must be applied, extreme care should be taken to ensure that no undesirable effects occur as a result.

4.5.3.4 Training

In all cases, it is recommended that the user's application engineers, as well as the appropriate personnel from the plant staff, attend formal training sessions conducted by knowledgeable manufacturer's personnel. This training should include features specific to the project application as well as to the manufacturer's hardware and software. The plant staff should also participate in the design and layout of the operator interface, if possible.

4.5.3.5 Data Manipulation

The additional facility of distributed digital control systems to manipulate data should be exploited to improve control over the process, and to enhance the image of the process presented to the operator. For example, operator interface displays should be linked to displays showing the control logic and its current status.

4.5.3.6 Power Plant Specific Algorithms

The system should be provided with pre-programmed algorithms specifically designed for power plant applications. These algorithms should be sufficiently developed as to require only the setting of certain user-definable parameters or tuning constants and the assignment of I/O to be fully defined. Examples of such algorithms include flow controllers with mass flow computing capabilities and "device" control algorithms with a complete set of motor and valve control and diagnostic logic.

4.5.4 Manual Control

The human operator is an essential link in the control of the plant processes. His intervention into the control system is through the manual control mechanism provided by the distributed system. The design of this interface should follow the principles of human factors engineering as described in sections 7 and 8

4.5.4.1 Manual Control Types

Manual control can be accomplished in several ways, and the applications engineer should evaluate the needs of the particular process and plant when making these choices:

1) Soft manual: This term refers to the facility to accept operator commands, through the shared use of an operator's CRT/keyboard station, transmitted across the data communications network to the data station where the command is output to the appropriate actuator.
2) Hard manual: This term carries two connotations:

Copyright © 1991 IEEE All Rights Reserved

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS Not for Resale

a) First, it refers to the use of a dedicated manual/automatic (M/A) selector station, similar or identical to those used in electronic analog control systems for the operator interface to the actuated device. This usage does not distinguish between M/A stations that are dependent upon the data station or data communications network, and those that are not.
b) Second, it is sometimes used to refer to dedicated M/A stations that are entirely independent of the control system; i.e., not dependent upon either the data station or the data network for operability (other than, in some cases, for power). In this case, dedicated cable from the control room M/A station to the associated field device is required for each hard manual station.

4.5.4.2 Design Philosophy for Manual Control

As a part of the definition of the control philosophy for the plant, the application engineer should establish which of these approaches to the operator interface is to be followed. Additional guidance on this topic is given in Section 7 Some considerations to be made in selecting the appropriate operator interface are:

1) Hard manual control, when not dependent upon the network, as in the second definition above, is not subject to interruption due to the possible loss of the network.
2) As hard manual control is operational without the use of a CRT, there is no need to call up displays or dedicate CRT screens before taking control action.
3) If loss of the network, or manual control without the use of CRT displays is intended, sufficient process data must be made available to the operator through means such as dedicated indicators to provide the essential feedback that his actions are having the desired effect. Such an arrangement can have a significant effect on system costs.
4) Soft manual control can be very flexible in arrangement, and can be arranged according to operational requirements without hardware changes. Revisions to hard stations typically require hardware changes.
5) The operator manual control station for a given final drive or manually controlled device can appear in multiple displays when the soft manual approach is taken.
6) In CRT based systems the operator will typically be at the screens during normal operation, and, depending on the arrangement of the control room and panels, may be able to respond through soft manual stations as fast or faster than through hard manual stations.
7) Advanced graphic display techniques allow the operator to manually intervene in the operation of the plant through process and equipment displays. A well-designed graphic interface is essential to this technique.
8) The use of a few hard manual stations for certain “critical” control loops or plant equipment is a frequently employed technique. Caution must be exercised in this approach to ensure that a coherent operator interface is established. Care should be taken to ensure that the operator is not forced to alternate between hard and soft stations. A simple, consistent, coherent, and logical operator interface is typically best. Use of an inconsistent mixture of hard and soft stations should be avoided.

4.5.4.3 Scanning Frequencies

For either hard or soft manual stations, and for all other operator manipulations to the system, the internal scanning frequencies should be arranged such that no change in the effected parameter (e.g., setpoint) occurs after the operator has released the push-button.

4.5.4.4 Control Action Access

Access to CRT displays from which control actions are to be taken should require a minimum of keystrokes. A means for providing this could be a group of dedicated push buttons. Direct access to the appropriate control screen from an alarm message is preferred.

Copyright © 1991 IEEE All Rights Reserved

--`,,`-`-`,,`,,`,`,,`---
Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS Not for Resale

4.6 Input/Output System

4.6.1 I/O System Functions

The I/O system provides the interface between the distributed digital system and the process. This interface may occur at the data station through an input or output module, or it may occur at the field sensor, as with systems using a field bus in the I/O system.

4.6.1.1 Dual Function

The I/O system has a dual function. First, to condition and convert the input signals from the process to a digitized format understandable by the system and to convert output signals from the internal digital format into signals that can drive the field actuators. Secondly, the I/O system performs a degree of preprocessing on the raw input signals before they are transferred to higher level functions.

4.6.1.2 Response Time

As a component of the overall system response time, the I/O system should provide very fast data acquisition and actuation of outputs. Information consistency is improved if all I/O are scanned within a very short time frame. Information consistency is a term that refers to the degree to which current data in the systems memories is simultaneous, and is an attribute necessary for meaningful interpretation of that data.

4.6.2 Hardware Considerations

To effectively serve power plant control applications, the I/O modules should exhibit the following capabilities:

1) Modules should be environmentally hardy (see 4.7).
2) Modules should be available to accept all required signal levels and all modules should reject the common mode voltages that might appear between sensor ground and A-D converter ground.
3) All I/O modules (analog and digital) should be designed to meet IEEE Standard 472-1974 Surge Withstand Capability (SWC) Tests.
4) Manual adjustments or calibrations should be minimized by automatic calibration, automatic zeroing, and automatic ranging of the modules.
5) As with all printed circuit cards in the system, the I/O modules should be capable of installation or removal with the backplane energized, and without disturbing adjacent cards or field wiring. The modules should be designed in a manner that will prevent damage or misoperation if they are installed in the wrong cage slot.
6) Each individual signal, or group of related signals, whose simultaneous loss can be tolerated, should be protected to avoid loss of multiple inputs or outputs on a fault. Where signals are fused, all fuses should be accessible for inspection and replacement without removing the module from service. It is suggested that the distributed system monitor the status and alarm on the loss of any critical fuse.

4.6.2.1 Sensor Redundancy

Double or triple sensor redundancy should be considered for instruments used for critical process inputs. The acquired information should be verified and validated. Triple redundancy with median select software is preferred for the additional security provided, but is not always economically attractive. In nonredundant cases or cases with only double redundancy, measurements can frequently be verified by indirect methods.

4.6.2.2 Sensor Input Quality

The I/O system should evaluate the quality of the incoming signal from the field transmitter or device. Immediate reporting of bad quality should permit higher level programs to take corrective action. The I/O system should:

Copyright © 1991 IEEE All Rights Reserved

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS Not for Resale

1) Verify that the signal is within the valid sensor range for the variable, preferably, a range that can be dynamically modified to suit the operating mode of the plant.
2) Where appropriate, detect open or shorted field wiring, or failed coils, without adversely effecting the function of the field device.
3) Where practical, and without degrading their functionality, evaluate the health of the connected field devices. Developments such as the use of microprocessors in field devices will make this a very practical task. Likewise the I/O system should have sufficient intelligence to detect a blown fuse or a failed coil in a field actuator.
4) Take immediate corrective action to avoid any upset to the controlled process on detection of a failed control input, and notify the operator of the failure.

4.6.3 Interface Considerations

The application engineer should carefully consider the details of the interface between the control system I/O modules and external devices. Care should be taken to ensure that the electrical characteristics and constraints of the input and output devices are completely defined, and compatible with the external equipment to be connected to the control system.

4.6.4 Field Bus

In most distributed systems, I/O signals have been hardwired from field instruments to the cabinets that house the I/O modules. The signal level for this I/O is usually 4–20 mAdc for modulating signals. Development of a “field bus” (IEC TC65 SC65C WG6) or “field instrument network” (ISA SP50) provides another alternative for the applications engineer. This high connectivity, low level subnetwork links multiple instruments equipped with digital communication capabilities to the data station over a softwired shared communications medium.

4.6.4.1 Device Level Processing

As field devices continue to incorporate microprocessor technology, more preprocessing of data can occur at this point. At the same time, use of the field bus with these instruments eliminates the need for a digital to analog and subsequent analog to digital conversion of the input signal, as is required when 4-20 mAdc signaling is used.

4.6.4.2 Distribution

The principles discussed in 4.3 regarding physical and functional distribution apply to the allocation of signals to the various field buses that may be installed in a plant. The field bus provides a significant opportunity for savings in field signal wiring, but it should be applied with care.

4.6.4.3 Communications Security

The field bus, where used, should meet all of the requirements for a highly secure, dependable, and fast communication system, as outlined in Sections 5 and 6

4.6.5 Data Acquisition and Preprocessing

The I/O system provides a major portion of the input to the data acquisition task performed by the distributed digital control and monitoring system. This task covers the broad category of the collection of raw sensor data and the conversion of this data into useful information. The first step in the conversion process takes place in the I/O system through preprocessing. This preprocessing typically includes:

1) Signal conversion from metering units (ma, mv, resistance, etc.) to engineering units
2) Signal validation (within the appropriate range of values for the particular sensor)
3) Signal reasonability checks (within the appropriate range of values for the process conditions)
4) Signal linearization and scaling

Copyright © 1991 IEEE All Rights Reserved

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS Not for Resale

5) Alarm limit checking
6) Time tagging

4.6.5.1 Other Data Sources

The system database also receives data from other sources, both internally generated, as with system status checks, and from external sources, through gateways to other networks (if present).

4.6.5.2 Multiple Microprocessors

Some systems provide multiple microprocessors to perform the preprocessing functions, some perform these tasks within a multitasking, multiprogramming environment, in which a single processor (per card) performs multiple unrelated tasks simultaneously. The application engineer should take care to evaluate the dependability of these alternate approaches to the data acquisition task.

4.7 Environmental Considerations

Components of the distributed digital control and monitoring system should operate properly with no degradation in expected lifetime or in operational parameters in the normal power plant environment. The application engineer should carefully consider all extremes that the control and monitoring system may encounter during operation. Conditions during construction or installation should be considered as well.

All applicable codes and standards for safety, personnel protection, and application hazards should be carefully applied in the installation of the system.

4.7.1 Plant Environment

In any application of a distributed digital control and monitoring system, but particularly when the system is to be geographically distributed in the plant, variations in the operating environment should be expected and tolerated by the system. Where the environmental extremes exceed the capabilities of the selected system, the engineer should take appropriate steps to control the environment. The dependability of the environmental controls should be commensurate with the severity of the hazard, and the effects it may have on plant operation.

4.7.1.1 Temperature

It is reasonable to expect that a distributed digital control and monitoring system should be designed for operation in an ambient temperature range of 0 to 50 °C (32 to 122 °F). However, it should be noted that ambient temperatures above 35 °C and below 0 °C will generally reduce the life expectancy of electronic components. Self-heating will cause individual electronic components to operate at temperatures from a few, to tens of degrees above ambient. Likewise component arrangement in the manufacture of the system can have significant effects on local heating in the system.

4.7.1.1.1 Cooling

Cooling fans are a standard part of most systems. Special air conditioners are designed to fit on the walls of electronics cabinets when the required cooling can not be met.

4.7.1.1.2 Network Routing

Routing the network through high-temperature zones can result in degradation or destruction of the network medium. If this routing is necessary, then special high-temperature cable is available. Armored cable provides extra strength both for pulling in and for longer life. Use of metallic armor on fiber optic networks can, however, compromise the inherent immunity to ground loops and lightning strikes on a fiber optic network cable.

Copyright © 1991 IEEE All Rights Reserved

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS Not for Resale

4.7.1.2 Humidity

Many plants will see an ambient relative humidity range of from a few percent to 100%. In some locations, very low humidity environments can be encountered as well. To the maximum extent practical, it is suggested that the distributed system be designed to tolerate such extremes without external environmental controls. Where this is impractical the application engineer must take the appropriate steps to ensure proper environmental controls.

4.7.1.2.1 Condensation

Condensation should not be permitted to form in the cabinets, nor should water be admitted through conduit entering the cabinets from the tops or sides. Heaters may be placed in the cabinets to prevent condensation.

4.7.1.3 Atmospheric Contamination

Particulate contamination from fly ash and coal dust and gaseous contaminants such as SO_2 and other flue gas constituents can have deleterious effects on printed circuit cards, connectors, and components. Wherever possible this hazard should be accommodated in the manufacturer's design of the system. Where this is not possible the installation should incorporate the necessary atmospheric controls.

4.7.1.3.1 Filters

In cases where blowers are required to keep the cabinet electronics at reasonable operating temperatures, proper filters to remove airborne contaminants should be used and serviced at regular intervals.

4.7.1.4 Vibration

Vibration transmitted from plant equipment can cause connections to become loose, and can physically fatigue components in the system. The manufacturer of the system should include such features as locking devices, but the application engineer should ensure that the data station is mounted away from harmful vibration. Shock-mounting the cabinet is another, less attractive way of overcoming this problem.

4.7.1.4.1 Connectors

Since coaxial connectors can be loosened by internal cabinet vibration from cooling fans, they should be sealed.

4.7.1.5 Electromagnetic Interference

High levels of radio frequency interference (RFI) and electromagnetic interference (EMI) are normally found in the power plant environment. Portable radio transmissions, cellular telephones, and high magnetic fields are all found in the proximity of the distributed digital system's cabinets. Maintenance personnel will frequently use radios while working in the system cabinets. The system should be designed to be immune to such interference.

4.7.1.5.1 Cables

While fiber optics communications buses are immune to both radio frequency and electromagnetic interference, and shielded coax and twinax cables tend to prevent EMI and RFI, both the routing of these cables and system grounding are very important for optimum operation.

4.7.1.6 Static Discharge

Discharge of static electricity from tools or physical contact with electronic components can transfer sufficient energy to damage these components. Care should be taken to avoid such discharges through the use of wrist straps, antistatic mats, and the like.

Copyright © 1991 IEEE All Rights Reserved

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS Not for Resale

4.7.1.7 Lightning

If some of the stations are to be located outside of the main plant building, steps should be taken to minimize the effects of lightning strikes. Proper grounding, the use of spark gap lightning arrestors, metal oxide varistors, optical isolators and isolating transformers may all be necessary, and still may not provide complete protection.

4.7.2 Power Supply Considerations

The distributed system should include all power supply conditioning necessary to accommodate normal variations in the electrical supply to the data stations. Where the digital system is to be installed in power stations that may operate in an isochronous mode, care should be taken that variations in system frequency do not degrade system operation.

4.7.2.1 Power Feeds

The system should accept redundant power feeds for all stations. This redundancy should be continued in the external power supply circuits to the maximum extent practical.

4.7.2.2 Redundancy

Redundancy should be provided in the distributed system's power conditioning circuits.

4.7.2.3 I/O Considerations

The system designer should consider the action at the system I/O on loss and restoration of power to the field devices. Case by case evaluation is usually warranted to determine if, for example, measures such as dual outputs (start/stop) or external seal in logic are necessary for motor starters.

4.7.2.4 Field Wiring

Field wiring for contact interrogation or device control should be protected such that a fault on these cables does not cause loss of more than a minimum, tolerable, functionality of the system.

4.7.3 Grounding and Shielding Considerations

Proper electrical grounding is essential to eliminate noise, and minimize lightning surges. It is highly suggested that ac and dc power supply grounds are electrically isolated from each other and electrically isolated from the instrumentation ground. In addition, all grounds go to a single point on the grounding mat, if possible. IEEE Standards 588 and 1050 provide additional guidance on this issue.

4.7.4 Installation Considerations

4.7.4.1 Access and Serviceability

The stations should be located in areas where they are readily accessible for servicing. Adequate lighting and electrical outlets should be provided at these stations. The stations themselves should be designed for ready maintainability, as a low MTTR is important to dependability of the system (see Section 8). Control cabinets, printed circuit cards, and cables should be properly labelled to avoid operating or maintenance errors that could damage equipment or degrade human safety.

4.7.4.2 Security

In some cases, provisions should be made for cabinet security. Door locks are suggested for system cabinets, and a system mode keyswitch or password to prevent tampering with the program is also recommended.

Copyright © 1991 IEEE All Rights Reserved

--`,,`-`-`,,`,,`,`,,`---

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS Not for Resale

4.7.4.2.1 Redundant Elements

Redundant elements of the system should not be exposed to common hazards if possible. For example, redundant network cables should be routed through separate raceway to the extent practical.

4.7.4.3 Terminations

All physical connections in the system should be secure. This applies particularly to electrical connections. Field I/O wiring should be terminated with captive screw terminal blocks, separate from the I/O card itself to permit card removal and replacement without disturbing field wiring. The I/O terminations should be verified to be compatible with the plant's field wiring conventions for wire size and connector type.

4.7.4.3.1 Card Edge Connectors

Card edge connections should be protected from environmental contamination, and should include a locking mechanism. These connections should also be keyed to prevent improper installation wherever possible.

4.7.4.3.2 System Documentation

System documentation should identify every connection required in the system, including field I/O.

4.7.4.3.3 Accessibility

Considerations should be made in the selection of field wiring type and size, and in the selection of termination type, that there may be a large number of cables to be terminated at a data station. Appropriate space for initial wiring and maintenance access should be provided in the termination areas of such enclosures.

4.8 Documentation

As with all systems in the modern power generating station, the distributed control and monitoring system requires careful and complete documentation to facilitate initial system configuration, plant design, system installation, maintenance, training, operation, and future modifications. It is the intent of this section to provide only brief guidance in this area. Refer to Section 8 for a discussion of documentation applicable to reliability and dependability.

4.8.1 Design Documentation

The application engineer is encouraged to prepare a system block diagram, showing the allocation of functions in a hierarchical manner, circumscribing the tasks to be performed in the distributed digital control and monitoring system. When a specific system has been selected, this diagram should be modified to suit the particular architecture and distribution established for the project.

4.8.1.1 Effects

The effects of the use of a distributed digital control system on "traditional" documentation, such as logic diagrams, loop diagrams, piping and instrument diagrams (P&IDs), electrical schematics, termination drawings, etc., should be considered before a project is started. Standards are evolving to address the impact of distributed control on these drawings [B2] .

4.8.2 Level of Detail

Hardware documentation should be provided to at least the card level. Component level documentation is preferred, particularly for I/O cards, to provide the user with a thorough understanding of the system's capabilities and limitations. Some users will require sufficient detail to permit the user to manufacture replacement cards as protection

Copyright © 1991 IEEE All Rights Reserved

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS Not for Resale

against obsolescence. Protection of patent rights and licensing arrangements, as well as multiple sources for basic components, should be arranged in such situations.

4.8.2.1 Software Source Code

Software source code for all "application" programming should be supplied as a minimum. Source code for the manufacturers standard control algorithms, for specialized subroutines (e.g., steam tables), and for other "system" software will prove useful to users who intend to exploit the system to its fullest capabilities. Again, licensing agreements should be obtained with the manufacturer or third party software developer.

4.8.2.2 Revision Control

The reader is cautioned that the rapid evolution of microprocessor technology applied to process control systems often causes a gap between a system's hardware and software and the accompanying documentation. All documentation should be identified as to the particular revision or version of hardware or software to which it applies. Printed circuit cards should be identified, both on the card and in the documentation, as to the revision level of the card. Embedded firmware coding to permit the system to identify the hardware revision level through software is encouraged.

4.8.2.3 Software Update program

The system manufacturer should provide a software maintenance program accessible to system users. This program should provide for optional and, where necessary, mandatory software upgrades for systems in the field. Care should be exercised that any upgrades are fully documented and tested for use in the system as configured. After upgrades the user should be wary of unforseen problems that occasionally arise.

4.8.3 Self-Documentation

The distributed digital system should include the capability to provide both graphical CRT displays and hardcopy documentation, clearly defining the current status of the application software in the system. Desirable features in self documenting systems include:

1) Industry standard symbology and drawing formats;
2) Facilities to accommodate user comments and explanatory notes within the documentation;
3) Cross references to all other uses, both control and monitoring, for each data value within the system;
4) Revision control, including identification of the person initiating a change, revision dating, etc.

4.8.3.1 Self-Documentation Level of Detail

System self-documentation should be sufficiently detailed to permit a clear understanding of the control logic or signal processing being accomplished, and should be suitable for troubleshooting. The documentation should show not only the type of control, e.g., P-I-D, but should also show the controller tuning parameters, timer settings, etc., and physical data such as the data station in which the control is performed, I/O termination information, and so forth. On the other hand, the documentation should be clear enough to permit an understanding of the control scheme being reviewed, without being obscured by the details.

4.8.3.2 Maintained Hardcopy

The plant should maintain a current set of system documentation in hardcopy form at all times, to serve as reference if the system self-documentation capability is ever out of service. Likewise, prudence dictates that the utility maintain current backup copies of all system software, and maintain tight control over revisions to this software.

Copyright © 1991 IEEE All Rights Reserved

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS Not for Resale

4.8.4 Digital Documentation Storage

Advances in mass memory devices including the use of optical memory storage devices with very large capacities, make the use of digital techniques attractive for documentation storage. Documentation storage and retrieval systems using these techniques are already commercially available. Use of such hardware will enable plant personnel to have ready access to any plant documentation he may require, by storing this information digitally, and making it available to the plant data network. Particular care should be taken when extending the functions to be performed by the plant control system in this way. Additional functions should in no way degrade the performance of the control system in normal or abnormal operating modes. Various acceptable architectures can be envisioned to provide the functionality described above ranging from fully distributed documentation files resident in local data station memories to a centralized documentation file server in a centralized utility computer system, with a link to the individual plant and unit control data networks.

4.8.4.1 Interactive Links

Interactive links to CADD systems can provide a mechanism for maintaining current documentation as the control system evolves, and can also make all plant documentation directly available to the control room operator through his CRTs. Such links should be carefully designed and should not generally permit modification to data files through the control operator’s station.

4.8.4.2 Plant-Wide Databases

Through digital storage of documentation, relational plant-wide databases can be established such that the operator, engineer, or maintenance manager can rapidly access all documents related to a particular plant component. This facility can help to ensure that all documentation remains concurrent, by replicating a change in one document to all other associated documents.

4.8.4.3 Capabilities

These capabilities should be considered for documenting plant components and systems not otherwise associated with the distributed digital control and monitoring system, to obtain the benefits of rapid access, and relational associations. Schematics, instructions for vendor equipment, piping diagrams, etc., can all be included in a plant-wide documentation system.

5. Data Communications Structure

This section of the application guide discusses the data communications scope, functions, characteristics, requirements, and assessment in order to support distributed control and monitoring of power plant systems. Through an understanding of the data communications structure and requirements, the application engineer can better evaluate system alternatives.

5.1 Scope and Purpose

The data communications structure with regard to the intraplant (main) communications network and node protocols is described in this section. The various node architectures, subnetworks, and the application interface are covered in Section 6 The primary purpose of Section 5 is to define the stringent requirements that are needed to develop proper design specifications to accomplish the control data communication functions. These requirements focus on the real data communication needs for current and future power generating stations employing distributed control and monitoring, without attempting to either design a detailed system or promote an existing design from other industrial applications.

Copyright © 1991 IEEE All Rights Reserved

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS Not for Resale

5.2 Data Communication Functions

Future power generating stations will have a greater degree of automation and will employ digital technology to process the large quantities of data to support and enhance the human capability to monitor and control plant processes. The data communication functions that support distributed monitoring and control for this application are described below.

5.2.1 Control and Monitoring

The data communication network is used for transmitting time tagged measurement and status input signals to update live databases used by the distributed data station control and monitoring application programs. The application program outputs, consisting typically of control commands and alarms, are then transmitted in turn over the network to other data stations that interface directly with the process or that display or report information to the plant operators.

The data communication network is also used for transmitting sequence of event data with a specified time resolution. This data is recorded and displayed for trend and plant diagnostic analysis.

In the automation hierarchy (Section 4), the intraplant network services the unit and functional group levels. Subnetworks and field buses service the instrumentation and local control levels (Section 6).

5.2.2 Control Configuration and Initialization

Control configuration commands and data blocks may be transferred from the operator's console over the data communication network to the data stations. Additionally, application software may be downloaded through the network to the data stations to be stored in memory. The data communication network may also provide the means for transmitting tuning, calibration and setpoint parameters. These types of operations should be carried out under special authorization, guarded by either a special lockout key or access code.

Hence, the control data network should ideally support transfer of relatively long messages (e.g., file transfer) as well as relatively short messages for data acquisition reporting and control commands.

5.2.3 Network Management System

Other functions of the data communication network relate to the need to reduce operator and technician burdens to operate and maintain the overall distributed control and monitoring system. For example, hot and cold system initialization should be automatically achieved through the network management system, either automatically or by manual command from the control console.

Monitoring of network performance and status is another function of the system. Performance monitoring includes three components: performance measurement, which is the actual gathering of statistics about network traffic and timing; performance analysis, which consists of software for reducing and presenting the data; and synthetic traffic generation, which permits the network to be observed under a controlled load. This will allow the power plant engineer to assess the current status of the network, to locate bottlenecks and other problems, and to plan for future growth.

Network status refers to the monitoring function that keeps track of which nodes are currently activated and the connections that exist. This information should be available to the operator. The network also transmits specific diagnostic and maintenance troubleshooting data for status display.

5.3 Data Communication Structure Characteristics

The International Standards Organization (ISO) Open Systems Interconnection Reference Model [B7] provides a general structure for many data communication networks. This model describes a framework for developing data communication protocols in an orderly and comprehensive manner. The model separates the data communications

 Copyright © 1991 IEEE All Rights Reserved

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS Not for Resale

considerations into seven related groups of tasks or layers. Although the layers are not necessarily universally applicable to data communications for a process control network, reference is made to the highest layer and lowest two layers for the purposes of discussion in this application guide. The highest layer functions for the control data communications structure were described in 5.2.1 and 5.2.2. The lowest two of these layers, the data link layer and the physical connection layer, are discussed in more detail in this subsection.

5.3.1 Data Link Layer

The data link layer provides the procedures used to control the flow of messages represented as data in frames between data stations connected by the data communication buses. These procedures include execution of requested data transport services, control of data flow, control of station addressing, accomplishment of line access rules, synchronization of frame transmission, generation and supervision of error detecting codes, and control of error recovery.

5.3.1.1 Services

Generally, the control data network needs to support a number of types of virtual links: a link from one station to another station (dedicated); links from one station to all stations (broadcast); and links from one station to many stations (multicast). These links are employed, as is appropriate, to provide services such as send data with acknowledgment (SDA), send data with no reply (SDN) and request data with reply (RDR), etc. [B8] .

The types of services supported and the method for providing them will depend on the need for the specific services and the conceptual control data communication structure. For example, one effective way to implement a data link service of the type SDN is routine broadcast with only one address (the source) and fast synchronous transmission. On the other hand, if report by exception is used with an asynchronous transmission, SDA may be the most appropriate service.

Connection-oriented service is suitable for transferring blocks of data over the network for control configuration and initialization, but connectionless service may be preferred for routine data acquisition reporting, in order to avoid the overhead associated with connection establishment.

5.3.1.2 Media Access Control

Access methods can be generalized in a number of ways—for example, centralized vs. distributed, or statistical vs. deterministic—with various potential implementations possible within each classification to achieve the data communication functions.

In a typical centralized approach, a master station is designated and the other network stations operate as slaves to it. This approach may utilize polling and reservation techniques to gain access to the media, and may provide greater control over access for providing for such things as priorities, overrides and guaranteed bandwidth. Furthermore, coordination and logic at each station may be as simple as possible. But it may also result in a single point of failure or result in a bottleneck, reducing efficiency. Such a network often utilizes more overhead messages than other access control techniques and may have a longer response time.

With the distributed access approach, all stations have equal access to the media. Medium access is distributed using suitable protocols to the autonomous stations. While some distributed access schemes may be more complex than polling, there tend to be advantages in terms of fault tolerance, efficiency, and flexibility to accommodate modifications.

Distributed access may employ either statistical or deterministic access methods. With the statistical method, each station can transmit its data when it senses that the network bus is free. In contrast, for deterministic systems, a station must first gain approval through some coordination method before transmitting its data.

Copyright © 1991 IEEE All Rights Reserved

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS Not for Resale

The statistical method employs a simpler algorithm, provides fair access, and has good performance at low to medium load. However, it requires collision detection and has poor performance under very heavy load. A concern is that the system may be over-loaded in the case of plant or process upset, when many variables change, if sufficient load margin does not exist. Recently, many solutions to solve this problem have been found and practically implemented.

The deterministic method can provide excellent throughput performance and regulated access, but requires a complex algorithm. Special contingencies are necessary to prevent network hangup if coordination information should become lost during transmission to the network stations.

While numerous approaches are possible, (such as recover algorithms), each must be evaluated to assure that the basic requirements for control data communication (see 5.4 below) are satisfied. These requirements include response time, data throughput, data integrity, safety, etc., whose assessment must consider the particular power plant application under consideration.

5.3.1.3 Synchronous vs. Asynchronous Transmission

Synchronous transmission has all participating nodes of the control data communication network with a cyclic access to the medium. The frame format can be of equal fixed length or of variable length. The intermessage gap is fixed and very short. The senders and receivers are always synchronized; for example, through a special clock signaling line or self-clocking signaling. Nondata synchronizing bits are on the medium even during the interformat gaps. When the frame format is short, a synchronizing preamble can be avoided, resulting in a very efficient format [B9] .

An asynchronous transmission is characterized by sending messages only on a need basis. This need is established by the application layer. The format is of variable length. The sender and receiver must be synchronized during the preamble field propagation. For control purposes, the preamble typically has special nondata bits different from the nondata bits of the frame delimiters.

Synchronous transmission generally has a better data throughput and bit error rate, and provides guaranteed access to the medium under heavy load conditions. Asynchronous transmission regularly carries less numerous messages, but often of longer format. As a result, asynchronous transmission may have greater flexibility and is a better fit for file transfer tasks.

A hybrid approach has been proposed to capture the best features of synchronous and interrupted (asynchronous) protocols (see Section 6 and reference [B10]). In this scheme, synchronous time intervals, during which a fixed set of data is scanned, are alternated with time slots during which interrupts are accepted. Fast-changing variables are preferably updated by cyclic transmission, while very slow changing variables or rare events are transmitted during time intervals provided for this purpose.

5.3.1.4 Frame Formats

Current data communication systems for power plant applications employ bit serial data transmission. Data is embedded in a frame that may also contain synchronization, address and redundancy bits. Frame formats are typically optimized to achieve high data integrity with the lowest transmission and decoding delay times. This is achieved by using codes that achieve a specified Hamming distance (see 6.3.2.1) with the least number of check bits. In general, however, there is ultimately a trade-off between speed and data integrity.

5.3.1.5 Hardware/Software Considerations

Because network protocol processing can consume significant computing resources, there is often a processing capacity (one or more microprocessors or VLSI) for control data communication tasks and other processing capacity for handling the application programs. The data link/media access functions can be implemented in either hardware (VLSI or dedicated communications coprocessor) or software (operating on a general purpose microprocessor). In general, hardware solutions offer higher speed performance. Time decoupling of the propagation time and bit rate of the data flow from the node co-processors or microcomputers is accomplished using fast buffers and DMA controllers.

Copyright © 1991 IEEE All Rights Reserved

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS Not for Resale

5.3.2 Physical Connection Layer

The physical connection layer refers to network topology, and method of data signaling. Each of these topics are discussed further below. Discussion of physical media and noise immunity are also included.

5.3.2.1 Network Topology

Various topologies are feasible for data communications for distributed monitoring and control. These include the bus, ring, star, tree, and other systems that may combine these basic topologies. Each has merits and demerits that must be considered carefully to assure that the requirements for data communications, as expressed below (see 5.4), and the requirements for reliability and availability are satisfied.

5.3.2.2 Physical Media

Media type may include twisted pair, coaxial cable or fiber optics. Some factors to consider when choosing the physical media for a particular application include noise immunity, isolation characteristics, transmission bandwidth, signal attenuation, associated access methods, cost, installation and maintenance, and state of the technology. As discussed in 5.3.3, noise immunity is an important data communication requirement that requires a coordinated approach to the selection of many network design features and parameters, including topology, media, and signaling methods. When costs and maintenance are considered, the need for harmonious compromise becomes even more evident.

5.3.2.3 Signaling Methods

The signaling method of the physical channel can impact the error protecting capability and efficiency of the transmission considerably. Signaling codes fall into two main categories: carrier wave modulation and baseband.

Modulation signaling codes modulate a sinusoidal frequency, with changes to the carrier sine wave identifying the bit value. Modulation using frequency shift keying, phase shift keying, or amplitude shift keying is possible. Tradeoffs exist between bit density, reliability and ease of implementation between the three keying methods. Combinations of the modulation methods are also possible; for example, the use of frequency and amplitude shift keying in conjunction to achieve higher levels of reliability.

Numerous options for the choice of signaling methods exist. Frequency shift keying, for example, may be applied with a phase continuous method, in which a carrier wave's center frequency is modulated up and down to represent different logic levels, or a phase coherent method, in which two distinct frequencies are used to represent logic levels. Furthermore, a single frequency channel or multiple frequency channels (broadband) may be employed.

Baseband signaling codes directly impresses the bit pattern on the medium using electrical or light square waves. Many encoding schemes with their own data integrity and efficiency features are possible, but the tendency is to use Manchester codes. The encoding scheme selected should provide protection against dc drift and should have a high inherent Hamming distance. Another desirable feature is that the code be self-clocked.

5.3.3 Noise Immunity

Achieving satisfactory noise immunity requires a coordinated approach to selection of the physical connection layer features. Carrier-modulated signaling methods tend to be less noise-prone than baseband pulse modulated codes, but can be less reliable from other points of view and more difficult to implement. The noise immunity of baseband pulse modulated codes can be increased by using higher amplitude levels. Higher voltage levels for electrical pulse code transmission, however, means a longer rise time, which impedes the use of high frequency and may impact data throughput. Another approach is to use fiber-optic media, which is relatively immune to electromagnetic noise, but requires different components and topologies.

Copyright © 1991 IEEE All Rights Reserved

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS Not for Resale

Proper electrical grounding is essential to eliminate noise. It is highly suggested that ac and dc power supply grounds be electrically isolated from each other and electrically isolated from the instrumentation ground. In addition, all grounds should go to a single point on the grounding mat, if possible. Additional guidance on grounding can be found in IEEE Std 518-1982 [B11] .

Data communications for distributed monitoring and control, therefore, is seen to involve several subtle considerations of many issues that underlie the various computer networking techniques and multiplexing approaches. No one single characteristic can be employed to obtain a totally satisfactory solution. Rather, a harmonious compromise, based on long experience, may offer the best solution.

5.3.4 Network Layer

This layer is sometimes used in reference to communication between networks, either other local area networks or wide area networks. Communication between dissimilar networks requires the use of gateways that provide the necessary protocol conversions. In general, the use of gateways to transfer feedback signals for fast responding closed control is discouraged since such links may have high time delays that make it impossible to satisfy the time constraints. Where links are necessary between two networks, it is better if the networks can be connected by high speed bridges, which only need to implement the lowest two protocol layers of the ISO/OSI model; or the two networks, when serving autonomous control systems, should exchange only those signals that will not impact the response time constraints imposed by performance requirements.

There should be upward and downward compatibility with the intraplant control network. Upward compatibility includes provision for outside data links. These may include links to the management center, vendor technical assistance center and automatic power generation center, etc. Such links provide reports on control and diagnosis levels to management, but shall not allow inadvertent access to the plant control network.

Downward compatibility refers to the subnetworks, which shall have high inner connectivity. The subnetworks provide better geographical and functional distribution. They assure better fault isolation, faster processing, island stand-alone automation, and local logic for many purposes, such as alarm prioritization. The subnetworks are treated in more detail in Section 6

5.4 Control Data Communication Requirements

The control data communication structure requirements are presented in subsections below, according to the following taxonomy: Time constraints, dependability, safety, system transparency, and diagnostics and maintenance.

5.4.1 Time Constraints

Time constraints are a key consideration for specifying the data communication requirements. The information in real time databases should be a consistent image of the process. This means that there should be time and value consistency for each process variable, in the process, and in the database within a validity time. The acceptable error or resolution margin determines the validity time, which is variable with the variable rate of change of the particular variable at a particular time.

Additionally, quasi-simultaneity of the available information of all process variables involved in producing the process image for display and analysis is needed. The time resolution to satisfy simultaneity may be different from the validity time, and is denoted as the simultaneity skew.

Any analysis or display cannot be correct if it is not based on contemporary values. All components of the response time are of importance; for example, process variable sampling time, transmission scan time, processing time, etc., and all latencies should be kept very short. For the control data communications structure, the consistency and simultaneity relate to the response time and data capacity requirements.

 Copyright © 1991 IEEE All Rights Reserved

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS Not for Resale

Response time for the distributed control system is the elapsed time between the moment when a signal is originated in the input system of a data station until the moment the signal is available in an output system of another data station, assuming that the two stations are located in the worst communication situation possible.

Capacity refers to the maximum capability of the hardware and software of the network to communicate information in a defined time period. Capacity is related to the basic technologies employed and the effectiveness of the communication protocols for the network.

Response time and capacity requirements apply to the many types of data messages that must be communicated for distributed control and monitoring in the modern power generating station. Requirements are established for relational categories that include control and monitoring function classification as well as power plant system classification. Thus, there are requirements related to various types of control (e.g., modulating, logic, sequential, etc.), and monitoring, as well as specific plant systems, (e.g., turbine protection, generator protection, boiler control, coal handling, etc.).

5.4.1.1 Response Time Requirements

The total time budget for controlling and monitoring plant processes through a distributed system includes time interval subcomponents of signal conditioning and transformation in the input system of a data station, signal transmission over the communication network, and signal conditioning and transformation in the output system of another data station. It is possible that other data stations may provide the necessary transformations, in which case both transmission from the input system and transmission to the output system of the data stations interfacing directly with the process must be considered. Manual control also requires two transmissions over the data communication network, one for transmission of the operator's command, and the other for providing feedback response or confirmation of the command back to the operator.

Scanning requirements for the digital signals available for transmission from each data station provides an alternate and frequently used means to characterize data communication response time requirements [B6] . Scanning requirements may be stated in terms of the scan period, defined as the time between two successive transmissions of the same signal from the same data station or scan rate, or defined as the reciprocal of the scan period—i.e., the number of equally spaced scans in a given time interval.

The response time for data communications is guaranteed to be no greater than the maximum scan period for a given data transmission assuming a common destination. However, certain power plant response requirements are stated in terms of time to actuate after detection of a certain unsafe condition. For such cases, the scan period must be subtracted from the time budget available for all other equipment delays. This may lead to a relatively fast scanning requirement. Therefore, response time requirements are best established for two types of data messages—state data, for which scan periods may be specified, and event data, for which response time may provide the best specification.

The shortest response time capability is a fundamental characteristic of a network. A network can easily accommodate longer response time than its shortest response time capability, but the reciprocal is not generally true.

5.4.1.1.1 Scan Period Selection

Factors that affect the selection of a scan period include the type of variable, the type of sensor, the noise characteristics of the signal, the use of the signal, the actuation time of control devices, the criticality of the signal with regard to plant safety, and the time constant of the system process. Most likely, the designer will strive to select a limited number of scan periods, based on experience with the above factors, that optimize the overall plant data flow.

Response times for various types of control, protection, and monitoring in power generation stations based on a consideration of the factors listed above are provided in 4.5.1. While such ranges are typical, the requirements of control and technological advances tend to push these figures increasingly shorter.

Copyright © 1991 IEEE All Rights Reserved

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS Not for Resale

5.4.1.1.2 Digital Protection Logic

The turbine-generator, switchyard, and plant specific safety systems may require protective actions within a specified time of detection of certain unsafe conditions. In general, the data communications transmission speed should be an order of magnitude greater than the total time budget available for protective actions. Very fast transmission of certain logic or event data for protective actions may therefore be required for data communications.

5.4.1.1.3 Modulating Control

Response time and scan period requirements for modulating control are generally less stringent than for digital protection logic. Scan periods are frequently used to specify time constraints.

5.4.1.1.4 Manual Control

A desirable feature for manual control is that the operator should see a quick reaction to a command, in order to avoid irritation and human errors in perceiving the state of the system. On the other hand, digital displays that are updated too frequently can also be a source of irritation and confusion, as the operator has no time to distinguish the displayed value before it changes.

For manual control commands, the data communication system has to be fast enough to support the man-machine interface requirements of Section 7 The requirements for data communication speed can be derived by subtracting allowances for CRT update time and considering the fact that the data bus will need to be traversed twice, once from the operator station to the remote data station, and then from the remote data station back to the operator station.

5.4.1.1.5 Monitoring

For the purpose of analog and digital monitoring, a scan period consistent with those for modulating and manual control functions is generally adequate. The time processing requirements of automatic monitoring programs should also be considered.

5.4.1.1.6 Reporting

Reporting is the application function that brings information to the system and to the operators about the state of the process and events occurrences. For the state variables that are continuously evolving in time between limits, three attributes should be ideally reported: the value, the rate of change, and the time of sampling. For events, representing discrete variables that have only two states, the time of occurrence of change shall be reported. Events can be brought to the system knowledge either by a very fast sampling or hardware interruption.

The application of reporting can work in two ways: (1) “report by exception,” in which the reporting program evaluates the amount of change and the rate of change for a state variable, or the time of change for an event, and then decides whether to assemble a message for transfer to the data link level; or (2) “periodic report,” in which the reporting program routinely assembles the message, comprising state variables’ values or events with their time tag, and transfers it to the data link layer during each scan cycle. These applications employ the statistical deterministic methods for media access control, respectively, the merits and demerits of which are presented in 5.3.1.2.

Reporting by exception is event-driven reporting. It has the advantage of reducing the number of messages that wait to be transmitted. This advantage was very important with the early, low-capacity networks.

Reporting by exception is compatible with an asynchronous transmission, since the moment of transmission is established by the incidence of an event. In common practice it goes with a double address data protocol unit (DPU) format, which is source and destination addresses.

A potential disadvantage of reporting by exception consists of the disconnection between the sensors and the system when the variable values are between the lower and the upper preestablished limits. Consequently, the high resolution

Copyright © 1991 IEEE All Rights Reserved

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS Not for Resale

and accuracy of sensors are used by the system only when the limits are reached. In between, the variable values are supposed by the system.

Another disadvantage of this reporting consists of its related asynchronous transmission. The transmission of messages takes place at unknown intervals and sequences caused by prioritization of messages. The unorderly arrivals of data can make the control and monitoring functions difficult and less consistent (see also 5.3.1.3).

Cyclic (periodical) reporting reports fast moving variables in each cycle time; the slow moving variables are reported once in a couple of cycles (or more). This kind of reporting is used with synchronous transmission and routine broadcast.

The advantages of periodical reporting consist of the fixed intervals of reports, the guaranteed response time, even in the worst case, and the use of routine broadcast as an updated database located in the medium itself.

The disadvantage of periodical reporting consists of the requirement that procedures of the system be confined within a scanning cycle period—consequently, a fast network and fast computers are required.

5.4.1.1.7 Sequence of Events

Sequence of events time resolution shorter than 10 ms is often advocated, but practical experience has shown that such resolution may result in inconsistencies due to time delays not directly associated with control data communications; for example, the delays associated with mechanical contact closure for pressure, temperature, and limit switches, which may range from 20 to 50 ms. Continued technology progress in event detection, however, such as use of optical sensors, is expected to reduce time delay uncertainties. Furthermore, many utility companies request one millisecond time resolution for sequence of events, since it is generally within the capability of the control data communications structure to provide time granulation on the order of one millisecond.

5.4.1.2 Data Capacity

A control network needs to transmit both short messages for reporting and commands and long messages called file transfers (see 5.2.2).

For short messages, the most important feature is the number of data point transmissions per time. Capacity in this case is proportional to the number of various data points and the frequency of their transmission over the shared data bus. It is also proportional to the length of the various data packets, which includes both the data bits and overhead bits—for example, data point identification, addressing, error detection and correction, etc., required by the particular frame format.

For long messages, the most important feature is data throughput. Throughput refers to the number of bits of data information transmitted over the shared data communication medium in a given time interval.

A detailed analysis of the plant data flow, including categorization of data points and the associated number of signals, scan period, data packet lengths, etc., of each category, should be part of the plant design specifications in order to permit determination of the required data capacity for data communications. Databases for retrofit applications might typically have 500 analog and 1500 digital signals. More representative numbers for new power plants are 4000–6000 analog and 7000–9000 digital signals.

Sufficient data transmission capacity should be available to assure that critical data important to the safe operation of the power generating station is transmitted and received over the shared media within the time constraints and dependability requirements. Transmission of this data should be guaranteed for all operating modes, including plant upset conditions.

Copyright © 1991 IEEE All Rights Reserved

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS Not for Resale

5.4.2 Dependability

Dependability is another key requirement for data communications for distributed control and monitoring of the power generating station. Dependability is a broad term that captures concepts of quality, reliability, and availability.

Dependability and response time are two requirements that may be in conflict, and often a suitable compromise in the specification of these requirements must be achieved for the practical design. In developing such a compromise, however, the goal should always be to promote strong consistency between the process and its image as seen by the automatic controllers and the operators.

In this subsection, transmission error rates, accuracy, efficiency, and redundancy are discussed as related to dependable communication protocols. Further discussion of dependability issues, particularly as related to hardware considerations and total system configuration, can be found in Section 8

5.4.2.1 Data Integrity

The basic requirement of passing information correctly and quickly to its destination leads to data communication protocols that achieve specified data integrity levels by transmission of frames with minimum necessary code redundancy. This goal is achieved by imposing suitable block encoding and frame synchronizing on appropriate channel signaling methods.

5.4.2.1.1 Bit Error Rates

At the physical level, data integrity is determined by the influence of noise energy on the bit error probability. Increased noise immunity requires increased energy per distinguishable signal element that, with given signal levels, necessitates increase expenditure of time per transmitted signal element.

For low residual frame error rates, it is desirable to keep the raw bit error rate as low as possible, while still achieving suitable response time performance. An isolated raw bit error rate of one in a billion transmitted bits is a suggested goal in order to maintain high data transmission efficiency.

5.4.2.1.2 Residual Frame Errors

At the data link level, data integrity is determined by the number of bit errors that cause undetectable frame errors. Increased protection against such residual frame errors has typically been achieved through increased code redundancy—that is, redundancy bits for frame synchronization and error detection and correction, which results in longer transmitted frames, and again increases the transmission delay time.

The end user is advised to request theoretical and experimental statistics about channel error bit rate and residual error bit rate for proposed systems for a given application.

5.4.2.1.3 Frame Synchronization

In order to achieve specified data integrity requirements, the level of protection against undetectable message errors caused by synchronization slip should be equivalent to that achieved by the corresponding block error check sequence.

5.4.2.1.4 Signaling Methods

It is noted that protection against block code and synchronization errors also depends on the bit signaling method of the physical channel. Appropriate signaling methods should be employed in conjunction with block error and frame synchronization techniques to assure that the data integrity requirements are satisfied.

Copyright © 1991 IEEE All Rights Reserved

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS Not for Resale

5.4.3 Safety and Investment Protection

Safety and investment protection must be of high concern in the development of requirements for distributed control and monitoring of power generating stations. For data communications of distributed control and monitoring, safety means both the above-mentioned requirements and requirements regarding data capacity and functional survivability under plant upset conditions.

The consequences of plant upset and accident conditions on the data communication links in the plant should be understood through appropriate analysis, and sufficient contingencies should be incorporated in the design to assure safe plant operation and to protect plant investment. A single failure point should not cause the entire control data network to fail. Upon failure of specific data communication links or remote data stations, the overall data communication network should automatically reconfigure and continue transmission of data among the operable components without compromising plant safety and investment protection. The composite plant control design should be fail-safe; that is, if the network as a whole cannot operate, the plant will be automatically shutdown in safe conditions through automated island logic.

Furthermore, the control data network should comply with safety requirements regarding hazardous atmospheres, flameproof construction, and intrinsic safety, according to appropriate categories, such as those described in references [B12] to [B16] .

5.4.4 System Transparency

System transparency refers to automation of the control data network operations so as not to increase the burdens imposed upon the operator or to escalate the requirements for operator skills. Therefore, the data communication services, particularly with regard to such important functions as cold and hot system initialization, should be automatic and invisible to the plant operators, who must devote their attention to more important issues regarding the overall monitoring and controlling operation of the power generating station.

Configuration of the system should also be simplified as much as is practical, requiring a minimum number of inputs and commands on the part of the operator. When inputs are required, useful operator aids and guidance should be provided that minimize operator effort and required level of understanding of the detailed system design. Properly configured distributed control and monitoring should respond as one integrated system, without the need for operator awareness that the system is comprised of numerous separate computing entities.

5.4.5 Network Management and Maintenance

Network monitoring and self-testing and diagnostic intelligence should be built into the hardware and software of the data communications system, so that minimal interaction on the part of technicians and minimal downtime is required to determine the source of problems and the corrective actions needed. Failure analysis should also be done on self-diagnostic hardware and software to make sure these failures will not contribute negatively to safe operation or equipment damage.

5.4.5.1 Network Performance Monitoring

There shall be continual monitoring of network performance and status. The monitoring functions described in 5.2.3 shall be provided in order to allow the operator and power plant engineer to assess the current status of the network, to locate bottlenecks and other problems and to plan for future growth.

5.4.5.2 Error and Fault Supervision

Transmission quality and performance should be supervised and appropriate alarms should be provided upon determination of certain degraded conditions. Counting the number of rejected data frames or retransmissions, for example, can be monitored, with corresponding alarm indications when count rates become too high.

Copyright © 1991 IEEE All Rights Reserved

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS Not for Resale

Supervision of the network topology should also be performed on a continual basis. Changes in the topology caused by station dropout or initialization of new stations should be reported. Stations that improperly communicate on the media should be disconnected from the network. Reconfiguration of the network should be automatic and satisfy safety performance requirements.

5.4.5.3 System Maintenance and Modification

Greater system acceptance will also be achieved if flexibility for modifications and expansion capability exists and can be easily implemented without the need to bring the entire system down. Hot repair or system expansion should be possible, therefore, with the remaining parts of the network on-line. System reconfiguration following repair should be simplified and automated as per the discussion in 5.4.4 above.

5.5 Control Data Communications Assessment

For a proposed application of a distributed control and monitoring system for a power generating station, the application engineer may desire assurance that the control data network will meet specific system requirements, such as those listed in 5.4. Such assurance may be provided in a variety of ways through a number of means, and may include analytical evaluation of system performance, testing of prototype systems, and operating experience with a similar system in a related application.

System testing and operating experience provide good assurance of system performance, when such testing and operation is exhaustive and performed in a realistic manner and environment compared to that of the proposed application. A given application, however, may have unique characteristics or sizing requirements that will require test and operational data to be supplemented with certain analytical evaluations to show satisfaction of requirements for the proposed system.

Response time and data point capacity of the control data network are two important parameters for the application engineer to consider when evaluating a given system. The response time can be evaluated by summing components of the input delay time, scan time for the sending station, processing time for the sending node, media access time, transmission time, processing time for the receiving node, scan time for the receiving station and output delay time [B17] .

The input delay time is the delay before detecting input transition. The scan time for the sending station is the input update time, i.e., the program logic execution time, etc., and should be doubled in the summation to include the case where the signal changes just after the input update. Similarly, the scan time for the receiving station is the output update time, and should also be doubled in the summation of time components. The processing time for the sending node is the time between solving the program logic and becoming ready to transmit the data. For the receiving node, the processing time is the time between receiving the data and having data ready to be operated on by the program logic. The output delay time is the delay involved in creating the output transition.

The access time, which is the time involved between becoming ready to transmit the data and the actual transmission, and the transmission time, which is the time to actually transmit the data to the receiver, are determined by the characteristics of the control data network. These times depend on network characteristics such as media capacity, topology, access methods, frame formats, and communication protocols, as described in 5.3. Depending on the network, they might be derived easily from algebraic expressions, or a detailed simulation of the network using statistical network models and realistically queued data flow may be required [B18] . Such analyses may require the support of the vendor, who understands the characteristics and parameters of the network.

Data on capacity should be scrutinized carefully to determine the conditions under which the measurement was taken. The number of data signals that can be transmitted will vary depending upon the transmission scan rates and system loading. In power-plant application, different scan rates may be applied to different signals, and system loading will depend on the plant operating state; for example, normal operation versus plant upset. Detailed analysis may be required to show acceptable data communications under the various conditions.

Copyright © 1991 IEEE All Rights Reserved

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS Not for Resale

6. Network Architectural View

6.1 Introduction

While Section 5 is involved in general principles and requirements of a control data network, Section 6 assesses the options available for the network's nodes and subnetworks.

Section 6 consists of a supporting group of functions, pertaining to the Data Communications Structure.

Figure 3, semantic network of Section 6, shows how the I/O system is connected to the application interface and data acquisition functions. The application interface makes the liaison to the data station (usually the application interface is part of the data station, but sometimes the application interface belongs to the I/O system). When the application interface belongs to the I/O system, it makes the link to another kind of sub-network.

There are many ways of linking the field instruments to all control and monitoring hubs and ultimately to the highest (unit) control and monitoring center.

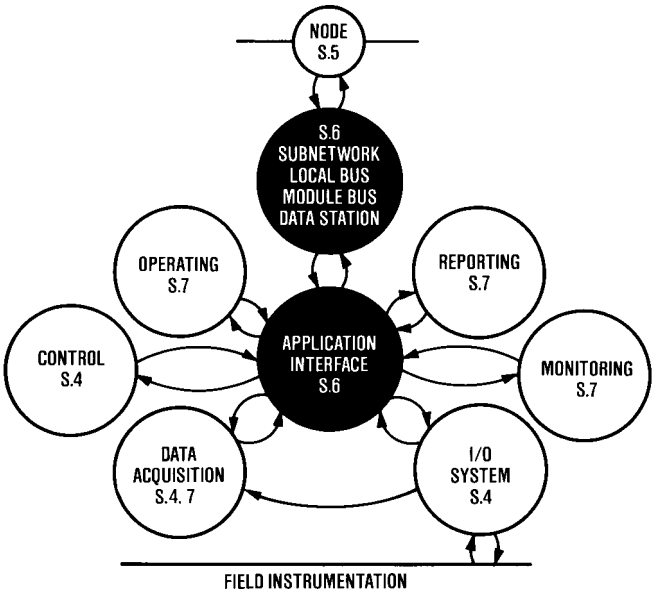


Figure 3—Semantic Network

Copyright © 1991 IEEE All Rights Reserved

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS
Not for Resale

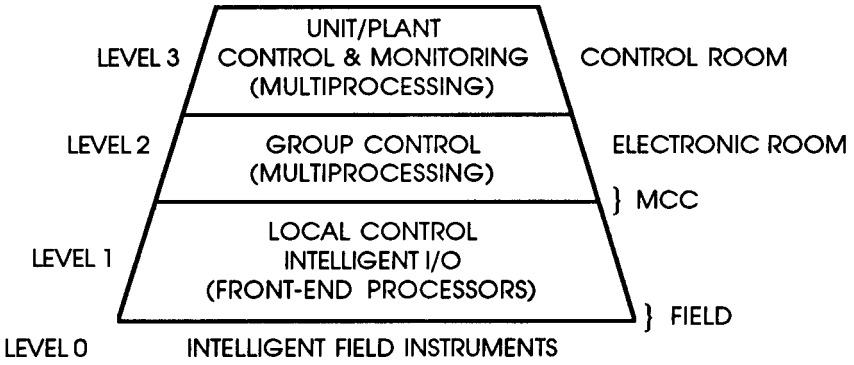


Figure 4—Control Hierarchy

The following subsections show some alternatives and their trade-offs.

The integrated control and monitoring system should be seen as a whole, beginning at the intelligent field instruments and ending at the unit control and monitoring center, structured in a functional hierarchy.

Figure 4 shows a simplified control (automation) hierarchy, which is an equivalent scheme of Fig 1.

A system as shown in Fig 4 should be based on an integrated control software, and modularly structured to fit distributed processing and the required application needs.

Such a system imposes more severe requirements on the data communications structure.

Since the number of end users and the geographical spread, which should be covered by the control network of the new systems, have increased dramatically, a single universally addressable and accessible network to meet the time and length constraints is difficult, if not impossible sometimes, to achieve.

An architectural solution should be adopted, exploring the present available options, that offers separate intraplant networks with sub-networks. Even more complicated architectures are considered by open (standardized) approaches. The performance and dependability became the major concerns of the control data networks.

A control network is composed of nodes (entities of communicating equipment) and the communication media that span the distance between nodes. The nodes can have various functions within the data communications structure as well as within the control and monitoring structure. A common function of all nodes is communication interfacing with the network to which they belong. The other roles of a node depend on network architecture and control/monitoring task mapping.

For power plant control the more severe requirements apply, because the power generation process is very costly and has potential for equipment damage. The following subsections of this section show some criteria by which to judge and select the best approaches for power plant control applications. These considerations, possibly, do not apply to other industries.

6.2 Remote Intelligence of Distributed Control Systems

A very important step toward an advanced control system is the increasing implementation of intelligence at the remote levels 0 (field instruments) and 1 (local control) (Fig 4). “Intelligence” is the programmable capacity embedded in equipment that improves its functionality.

Copyright © 1991 IEEE All Rights Reserved

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS Not for Resale

The availability of microprocessors made possible the implementation of intelligent electronics in the body of transmitters, actuators, conditioning, and I/O equipment.

The larger geographical distribution of hardware complicates network architecture and imposes more stringent time constraints, better software modularity and concurrency, sophisticated network management, and more stringent information consistency throughout the system.

Remote intelligence has the advantage of data reduction at the source, favoring a true distributed data processing among a large number of processors working in parallel, consequently reducing the communication bottleneck and improving distributed redundancy (see Section 8).

6.2.1 Rationale Behind the Intelligent Transmitter

The accuracy of field instruments affects the overall plant performance. Optimization techniques, obtained by automatic control or manual operation depends on measurement errors and information obsolescence. The measurement errors are caused by nonlinearities, lack of repeatability, hysteresis, zero drift caused by temperature and static pressure variations, drift in time, etc.

A microprocessor, embedded in the electronic equipment of the transmitter, can decrease errors by the following means:

1) Range changing to the full-scale value;
2) Algorithms that compensate automatically for temperature and static pressure;
3) Automatic and factory calibration instead of field calibration;
4) Diagnostics facility.

For more details see References [B19] –[B22] .

If the intelligent transmitter sends a signal through an analog 4–20 mA channel (over a pair of wires), there is a need of a double conversion (A/D and back to D/A), in order to install the microprocessor in between. The converters diminish the accuracy of measurement. If the signal is transmitted digitally through a field bus, the conversion is eliminated twice, first at the field instrument and second at the conditioning equipment. That generally means less cost, better accuracy, more reliability, and easier maintenance.

In some cases, the total measurement accuracy can be increased by a factor of five with intelligent transmitters [B19] .

Intelligent transmitter scales are much larger than those of conventional ones. The span turndown can be 10:1. Electrically erasable/programmable read-only memories (EEPROMs) retain identity, temperature signature, and transmitter’s constants during power outages. Accuracy of 0.05% of the reading are obtainable.

Using intelligence, the loop ranging is performed automatically. That means more accuracy with reading always equal to span. The control system can continuously monitor the validity of the measured variable. Remote trouble shooting and self diagnostics are possible through the control network from an operator’s console.

Through the digital connection field instrument-distributed control system, more information is available concerning diagnostics, maintenance, and autoscanning. With the increased number of sensors with accrued accuracy, more fluent information paths, and higher reliability, the process control, quality, and optimization are improved.

6.2.2 Intelligent Actuators

Actuators provide the muscles for process control systems. Until now, they have been limited to following the commands issued by computerized controllers. These commands between digital controllers and actuators have required cumbersome protocol translation and conversion of the controller’s digital messages into the actuator’s analog language.

Copyright © 1991 IEEE All Rights Reserved

--`,,`-`-`,,`,,`,`,,`---
Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS Not for Resale

Currently, there is a continuous actuation evolution from pneumatic and hydraulic to electric and electronic actuators. Microprocessor-based electronic actuators are increasingly being used.

Intelligent actuators accept digital commands and relieve the controller system of trivial tasks, such as the conversion from digital to analog and back, with the direct digital application of the regulating algorithm. They typically interface with field buses for connection to the entire distributed control system [B20] .

6.2.3 Intelligent Signal Conditioning Equipment

In between field instruments and I/O racks, a new generation of functionally complete signal conditioners has become available. The adjustment pots have been removed, which increases the reliability.

The A/D and D/A converters take less conversion time with better resolution. A/D commercial converters with 16-bit resolution and 3.33 μs total throughput are available. An 8-bit D/A converts 400 million words per second with 0.01% accuracy [B27] .

The use of intelligent conditioning equipment may eliminate the 4–20 mA signaling and analog multiplexing, if a field bus connects it to the distributed control system [B21] .

More building blocks, digital/analog signal conditioning and isolation, and termination panels include processor boards. These modules convert digital inputs from switches to TTL levels. The output modules convert TTL to high-level signals for driving circuit breakers, motor starters, solenoids, and other actuators. 2500 V isolation is a common practice. Signal conditioning is available in a wide range of inputs, including thermocouples, RTD sensors, millivolt, volt, and 4–20 mA. The included board controllers are used for a large variety of programs, such as corrections, diagnostics, control, and communications.

6.2.4 Intelligent I/O Equipment

While the intelligence of transmitters, actuators and conditioners belongs to level 0 of automation (Fig 4), the I/O intelligence belongs to level 1, local control of this hierarchy. This section will describe benefits from including intelligence at the I/O equipment, placed in proximity to the field instruments.

By placing process intelligence at every I/O point, control loops can run locally, at high speed, alarms can be detected, cleared, or sometimes acted upon without delays from hierarchical involvement. Better redundancy can be designed toward immunity from failure of almost any equipment (distributed redundancy, see Section 8). Data can be converted immediately into engineering units, if the resultant message length is not too long for a speedy communication [B22] .

The intelligent I/O approach incorporates control functions such as modulating, position, motor control, logic, and sequential control. Mapping the control functions among the closest points to the field instruments, regardless of their nature, several benefits are obtained such as more integrity of the entire system, more reliability, less data communication paths, less delays for better information consistency. The I/O control operates independently from the data acquisition cycle, but within its time constraints. The scanning procedure can be supervised by the I/O processor. The I/O processors improve network bandwidth and make easier system expansion.

6.2.5 Hardware/Software Functional Distribution

Besides the hardware geographical distribution that obliges the system’s hardware to be located in the strategic environments of the plant according to criteria that are shown in Section 4, there is also a hardware functional distribution. Hardware should support the software distribution. The selection of hardware follows a functional distribution. The software itself is functionally distributed according to the automation hierarchy. The software structure should take into account the hardware geographical constraints. Between hardware and software distribution there are inherent interactive constraints; that is, the software shall meet the hardware requirements (e.g., CRTs), the hardware shall meet the distributed software structured modules requirements (e.g., amount of memory, computation power).

 Copyright © 1991 IEEE All Rights Reserved

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS Not for Resale

6.2.5.1 Hardware Functional Distribution

The following paragraphs will show some hardware/software functional distribution criteria that have an impact on the network architecture.

The microcomputers embedded in the field instrument and conditioning equipment (level 0, Fig 4) are called “front-end processors.” Due to their control tasks, they are usually fast processors. The front-end processors should be capable of operating in harsh environments, to be able to withstand shock, vibration, extreme temperatures, high voltage transients, and electromagnetic interference. The node computers of level 2 and 3 should be located in environmentally protected buildings such as motor control center rooms, electronic equipment rooms, and control rooms.

6.2.5.2 Software Functional Consideration

Software distribution is the functional mapping of program tasks among the distributed hardware components (see Section 4). Advantage should be taken in distribution of software, from the fact that many control tasks are to some degree independent from one another. Carefully mating software distribution with system architecture, system integrators can capitalize on the inherent parallelism of program tasks [B26] . The targeted advantages consist of speed and throughput concurrently processing and data message passing through network.

Most of the processors are programmed in a high-level language. New languages have been developed, called graphically functional block languages, that can replace ladder logic and modulating graphic languages [B23] , [B24] .

The use of graphically functional block languages has merged programmable logic controllers with microprocessor-based controllers for modulating control into what is now called “microcontrollers” [B25] . The new programming languages consist of designing the flow charts on the screen, applying symbols or “macros” from the graphic memory library or user-built symbols linked between themselves by any kind of lines (horizontal, vertical, or bias), according to the signal flow.

The application software can be checked on CRTs with color graphic displays.

The integrated control software should be designed as a real-time operating system (OS), or as a control programming language, except for the fact that it is distributed across the network, which acts as a software bus (from here comes the term “softwiring” as opposed to “hardwiring” (see Section 2).

The network architecture should be chosen based on the option that really fits each application.

6.3 Single Linear Network Topology—Data Station Architecture

A linear network topology is a simple communication bus, no ramifications, no subnetworks, on which simple nodes, in this case simple data stations, are connected.

6.3.1 Network Node Functions

The control network nodes may have different communications, control, and monitoring functions.

The nodes must implement the functional and geographical distribution of control system strategy. A perfect match must exist between the nodes’ functionality and the network communication features in order for a system to meet the process control requirements.

Copyright © 1991 IEEE All Rights Reserved

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS Not for Resale

6.3.1.1 Node Architecture

There are simple nodes (comprising only one data station) and there are complex nodes consisting of a link to a subnetwork.

The simplest node architecture consists of a communication interface linked to the network and an application interface linked directly to the dedicated control and monitoring hardware/software. Such a node is called a data station.

6.3.1.2 Data Station Architecture

Concerning the functions related to communications protocol, the well-known ISO/OSI model has had a heavy impact on many data networks. This model had been developed initially for wide-area packet-switching networks, with a meshed topology, telephone lines, and a store-and-forward media access control (MAC).

Influenced by the OSI model, the IEEE 802 standards conceptualized a model for local area networks (LANs) [B28] .

In Fig 5, reference is made to the IEEE 802 data station model [B28] , for clarifying general services involved in the network protocol of a LAN, Fig 5 shows that the OSI link layer (No.2) was subdivided into two sublayers; i.e., the logical link control (LLC) and the medium access control (MAC).

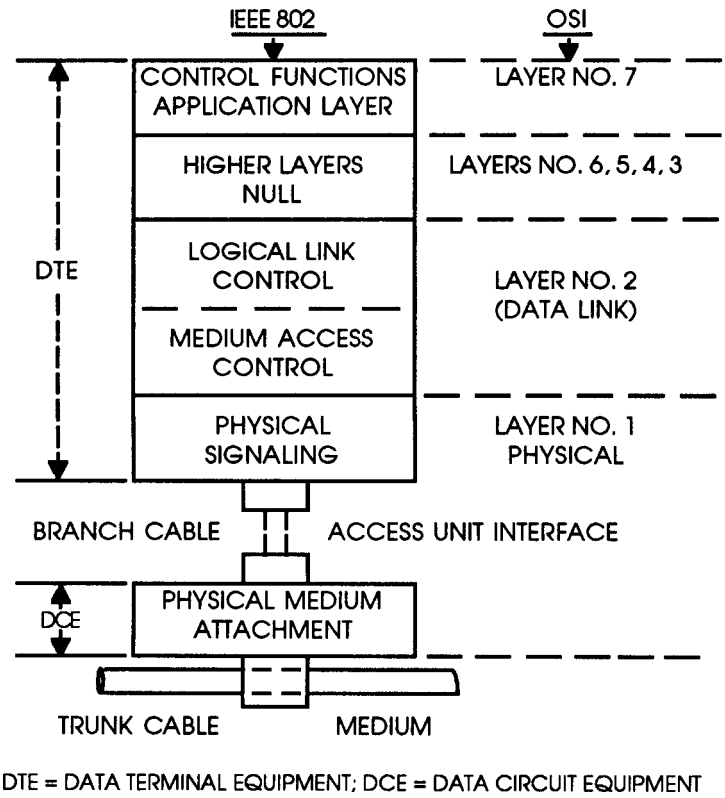


Figure 5—IEEE 802 and ISO Models

The IEEE 802 standards addresses only the two lower layers of the OSI model, namely data link and physical. For servicing the other layers, link service access points (LSAPs) have been defined.

Copyright © 1991 IEEE All Rights Reserved

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS
Not for Resale

The protocol layers are physically implemented by two major equipment components, data terminal equipment (DTE) and data circuit equipment (DCE), as shown in Fig 5. DTE comprises the hardware processing the layers' functions, including application programs, and it is installed inside a station cabinet. The DCE is attached to the medium.

6.3.1.3 Physical Implementation of Nodes with One Simple Data Station

Although all commercial distributed control systems depart more or less from the standard station model (Fig 5), some of them come closer by adopting a simple single data station within a network node.

Two basic approaches to station architecture are illustrated by Figs 6 and 7.

Figure 6 represents a physical implementation of a data station based on system bus. All modules, such as processors, memories, the network interface, I/O processors and modules, are linked to the system bus (usually a bit parallel bus). The functions of the network interface are shown structurally by Fig 5.

Figure 7 represents a dualport memory approach. The network interface comprises a dualport memory that allows access to the memory of both processors, one embedded in the network interface, dedicated to the communication chores, and the other, the functional processor, devoted to the application programs. Information to the application programs from the network and the converse, information from the local programs to the networks, are stored in the dualport memory.

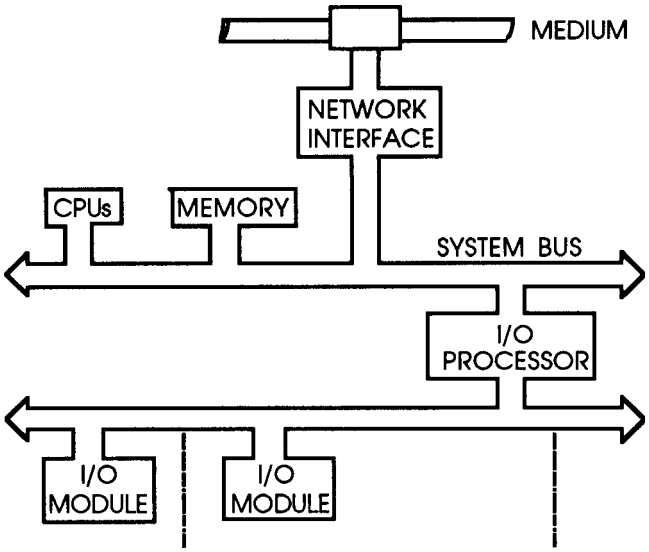


Figure 6—Physical Implementation of a Data Station Based on a System Bus

Copyright © 1991 IEEE All Rights Reserved

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS
Not for Resale

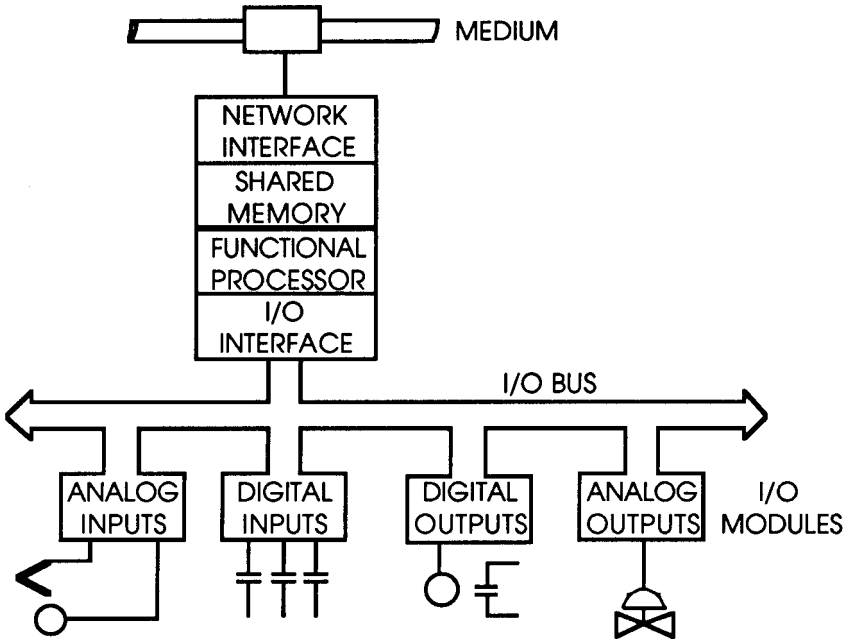


Figure 7—Data Station Physical implementation Based on a Shared Memory

6.3.2 Structure of a Linear Bus Architecture

An early concept of control network layout was the implementation of simply single specialized data stations located in protected areas, interconnected by a redundant linear bus. The entire plant should be covered by a winding single bus segment (redundant) (see Fig 8).

The advantages of the linear bus architecture consist of:

1) Simplicity
2) Ease of network management
3) Simple control reconfiguration.

The disadvantages of this topology consist of:

1) Long I/O hardwired connections to the field instruments, if the bus configuration is not used for a field bus or in connection with a field bus
2) If too large a number of stations are linked to the bus, the response time becomes too long
3) In some applications, lack of optimization of the data paths for distributed processing and automation hierarchy could appear if careful network architecture is not considered

Improvements of the linear architecture are possible by adding some kind of subnetworks. Such architectures are analyzed in 6.5.

In the following section subdivision, two network linear architectures are discussed, one open (standardized) and one proprietary.

Copyright © 1991 IEEE All Rights Reserved

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS Not for Resale

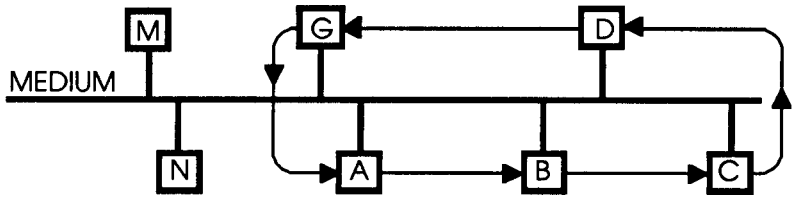


Figure 8—PROWAY Topology

6.3.2.1 PROWAY's Approach

PROWAY—an international and ANSI standard—is a dedicated network for control. PROWAY-LAN's basics are similar to a regular LAN of a bus topology (see Fig 8), with some additional features to adapt a regular LAN for control purposes.

PROWAY is an asynchronous transmission network (see Section 5), based on a communication session between a node A and a node B, with double address field, source, and destination. With these basic attributes, PROWAY is an event-driven network fit for report-by-exception (see Section 5). The PROWAY-LAN presents a data station architecture illustrated in Fig 9. The general architecture is compatible with the ISO/OSI reference model. The general architecture does not represent all improvements made by PROWAY to respond to control requirements. One of them is the vertical layer (Fig 9) representing the distributed network management function (see Section 5). Distributed, rather than centralized, network management is an essential function for the control network's safety. Figure 8 shows the PROWAY's token rotation among "initiator" stations (A, B, C, D, …, G). According to PROWAY, there are stations that do not initiate communication sessions. They are called "responders." An initiator (master) when it owns the token, will address a responder, which never receives the token (stations M, N in Fig 8), with such messages as send data with acknowledgment (SDA), request data with reply (RDR). During the transaction of such messages, the transmission over the entire network is frozen. Some overhead token-passing messages are spared, but the medium bandwidth is shared by responders and initiators. The transaction time (prime message processing response) becomes longer with the responder processing time, and any other transmission is stopped, which makes for long response times.

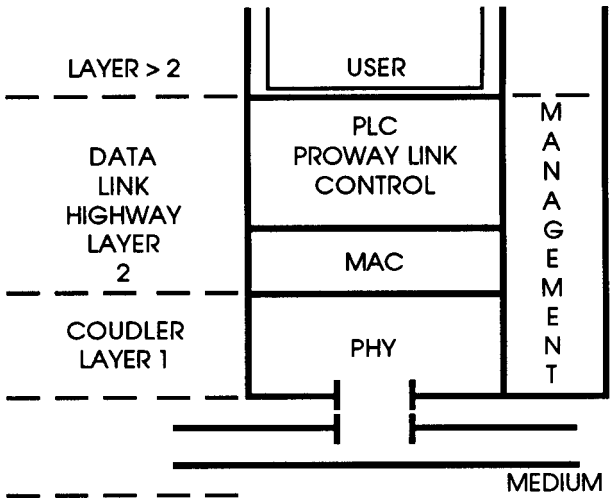


Figure 9—PROWAY-LAN Model

The token-passing MAC requires a large number of overhead formats, such as pass the token, acknowledge receipt token, claim token, initialization, lost or double token recovery, request data, acknowledge data, etc.

Copyright © 1991 IEEE All Rights Reserved

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS
Not for Resale

PROWAY-LAN's decentralized search for the token successor, when a station has been taken out for hot repair, may take a long time [B29] , [B30] , [B41] , as compared with time constraints of power plants' control.

The prioritization of messages is mandatory for an asynchronous control LAN. Any kind of prioritization, at the level of local control stations, is of little effectiveness. At this level, a nuisance, or a consequent alarm can not be discerned from a prime alarm message.

PROWAY's access time, as of all other token-passing LANs, is variable. The access time becomes longer in the cases of process/plant upset, because a majority of stations have numerous first- and second-priority messages to send out.

PROWAY IEC has the advantages of a physical layer designed for an industrial environment: Hamming distance of four (the Hamming distance is the least number of corrupted signal elements that may generate an undetectable word or frame error), a very low bit error rate, and a frame format corresponding to industrial requirements. The SDA and RDR are big improvements of data link services of layer 2. The redundancy of the medium is considered. The network management is favorable for industrial applications. PROWAY may be used as a control network for level 3, or eventually levels 2 and 3 of the automation hierarchy (see Section 4 and Fig 5), where levels 0 and 1 are served by field buses (see 6.5).

Concerning the OSI layer No. 1 (Physical), there is not yet enough experience to tell which is better between PROWAY 1 Mbps continuous phase and IEEE 802.4's 5 Mbps phase coherent carrierband signaling methods. Practically, 802.4's carrierband has the advantages of simplicity, speed, and lower cost. But some experts are of the opinion that continuous-phase, Manchester encoded (PROWAY IEC) is safer.

6.3.2.2 Proprietary Linear Architecture

This particular architecture is illustrated by Fig 10. It has been chosen because of its unique features.

The system is comprised of specialized data stations with equal right to access the bus (the medium is a typical bus topology). Figure 10 shows one box for more than one data station; e.g., the boiler has 12 stations for control and monitoring purposes.

The stations are functionally specialized as follows:

1) Combined control and data acquisition
2) Combined modulating and logic/sequential control
3) Global database management
4) Preprocessing for value conversion, value checking, alarm limits
5) Sequence of events recording
6) Switching software-wise from automatic to manual and vice-versa
7) Computing capacity
8) Operator's console
9) Engineer console

The specialization of data stations requires the capability of station hardware reconfiguration, I/O flexibility and expansibility, and software downloading capability.

The network data link control is cyclic reporting based. The synchronization of cyclic actions is ensured by a triple-redundant time clock central station. The cycle time is 100 ms, and it is divided in two phases: the first phase is for cyclic reporting (broadcast messaging with only one address), the second phase is reserved for special messages with two addresses. In the first phase, the address gives the right for the following station in the logical ring to send its cyclic report. This is unique token-passing that avoids the need of a bus arbitrator, but causes other disadvantages (see 6.3.2.1).

Copyright © 1991 IEEE All Rights Reserved

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS
Not for Resale

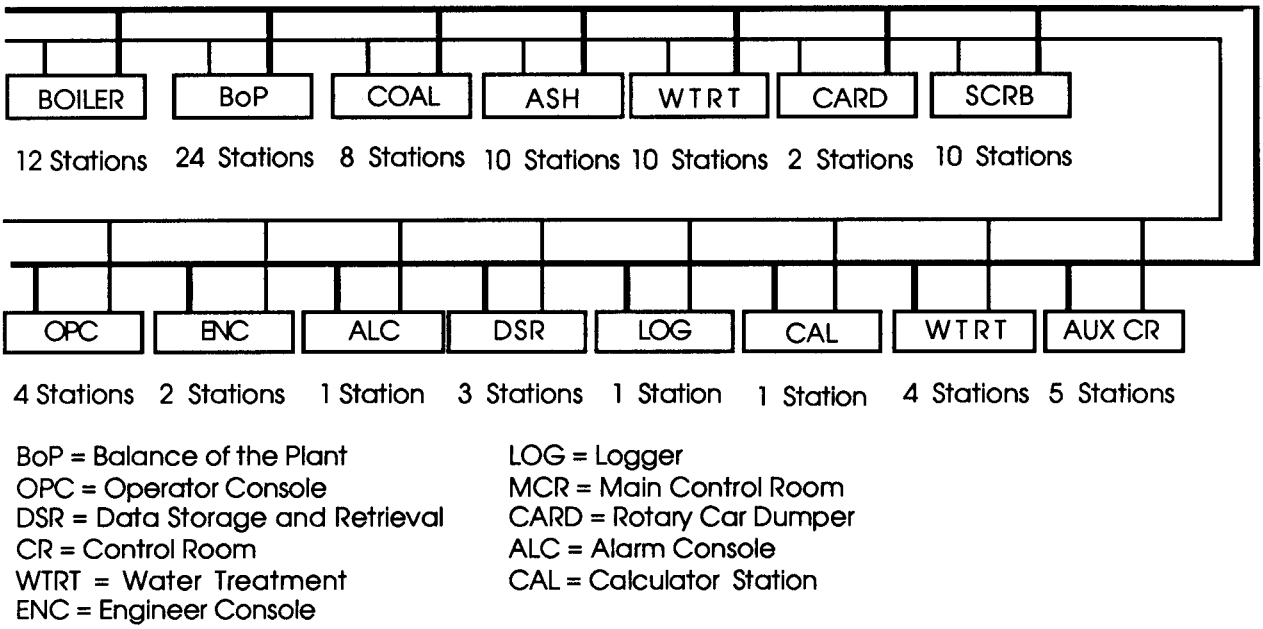


Figure 10—One Bus, Single Data Stations

The main advantage of this proprietary system is its cyclic broadcast reporting that has the potential capability for better information consistency. The buses are redundant, as are the master time stations. Any station is switched automatically from the faulted bus to the redundant bus. But its linear architecture has advantages and disadvantages as cited in 6.3.2.

6.4 Some Special Features of Proprietary Control Networks

The distributed control systems currently available on the market have communication structures supported by various technical features. The differences in their approach include:

1) Topology
2) Data link services
3) Medium access control (MAC)
4) Data protocol unit (DPU)
5) Subnetworks
6) Signaling methods

It is not the intention of this section to describe and analyze each system in detail, because most manufacturers continually improve their systems.

In this subsection, only general comments are given, concerning commercially available distributed systems, their evolution, and their features.

6.4.1 Topology and Medium

Among distributed digital control systems, there are two main network topologies: the bus topology, and the ring topology. The master to slave (active star) topology is less frequently utilized for distributed control of power plants.

Copyright © 1991 IEEE All Rights Reserved

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS Not for Resale

The bus topology has an advantage of bidirectional transmission. In a bus configuration, each node is attached directly to the communication media through appropriate interface hardware. Messages can be broadcasted simultaneously to all stations (broadcast media).

The ring has an advantage of accommodating longer distances. In a regular ring configuration, the communication media is connected in a point-to-point manner to each node, with each node acting as a repeater. This means that bidirectional communication cannot be accommodated, since the "transmitter" on one node is connected to the "receiver" of the next node (sequential media). This makes the ring system favorable for optical fiber transmission, since optical fiber is inherently unidirectional.

It is well known that optical fiber has some advantages when used in a noisy environment such as a power plant. Since the direct communications are only node-to-node, a ring system will allow a mixture of both optical media and coaxial media. This can be particularly advantageous when it is necessary to have only part of the communications media located in a noisy environment.

The delay caused by retransmission of messages at each node depends on the technology and design used by each manufacturer.

It is important that in any installation, careful fault tree analysis should be implemented that considers the action of the communications “network” under various failure modes. Such an analysis must consider both the topology and the protocol implemented to adequately resolve the issues.

As an example, one type of failure is a break in the communications media. In this example, a ring topology cannot transmit past the node preceding the break, since it is a unidirectional communications methodology. As a result, most ring configurations use redundant media. In some systems the redundant media is active on a full-time basis to prevent latent failures.

The bus architecture, if it supports bidirectional communications, transmits in the other direction to minimize the impact of this type of failure. Bus architectures may also rely on redundancy and separation to minimize this type of failure.

No matter what topology is chosen, there are electronics that will connect to the communications media. In the ring topology, if the node fails or loses power, it is necessary to bypass the node, or else the ring is broken. This may be handled by a mechanical relay. In this mode, the node is bypassed as if it were not part of the ring. Other solutions use optical switch, loop-back hardware, and software in neighboring nodes to isolate and bypass the failed node.

With a bus topology, loss of power or failure of the node has little impact since the node simply ceases to communicate. In either case, ring or bus, the network management must recognize loss of communication to the node, and provide diagnostics and information to service personnel to effect repairs.

Another type of failure is that the electronics that tie to the media fail in such a way that a signal is held high or low. This essentially brings the communications down, since no device can now communicate. With the ring topology, other nodes can recognize this condition and force a reset of the media such that the node is bypassed. This isolates the faulty electronics from the communications network so that the failure involves only the loss of the faulty node. With a bus topology, incorporation of "jabber" circuits are required to isolate the faulty node from the bus.

6.4.2 Network Architecture for Plant Geographical Distribution

Section 4 shows the criteria and requirements of the geographical distribution. Examination of the variety of network topologies and node configurations is required to assure good plant control coverage. The control network general design (including node architecture and subnetworks) provides the capability and flexibility to distribute the functional modules and/or data stations in accordance with the plant architecture and size. The fitness to the plant layout is a main feature of a distributed system.

Copyright © 1991 IEEE All Rights Reserved

--`,,`-`-`,,`,,`,`,,`---

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS Not for Resale

A number of solutions to the plant control coverage problem has been offered by control manufacturers. Some of these are mentioned below.

Only one single linear topology has been referred to in 6.3.2.2.

Some systems link a field bus to their nodes [B34] . Such field buses make a dedicated connection from an instrument to a node of the main bus. If these kinds of field buses are of sufficient capability and length to connect the field instruments to controllers, they fulfill the goal of a true field bus. But some systems confine the bus to a cabinet, which must be installed in protected areas.

In another approach to the geographical plant coverage, the main cables of fiber optics are interfaced to coaxial cable; this allows the easy attachment of some tens of data stations, mounted relatively close to one another, to the coaxial cable. This solution may impose some constraints to the search for the best geographical distribution.

To solve the control coverage of the entire plant, some systems segment the plant; e.g., the steam generator, the turbine-generator set, cooling tower, and scrubber. Each segment (island) of the plant has its own main network (either a bus or a ring). The network segments are linked together by a central computer facility that unifies the entire plant main network and operator supervision (see more details about this architecture in 6.5). Such a solution avoids a complex network hierarchy.

Another solution is the use of a network hierarchy where the hierarchical networks are linked through gateways or bridges (see 6.5).

An analysis of the best plant control coverage should be performed for each application case.

6.4.3 Data Link Services, Frame Format, Signaling Methods

Concerning these protocol features, again we encounter a large variety of proprietary approaches.

Historically, most of the data link services consisted of connectionless acknowledged change of messages between two nodes. Each change of messages between two nodes took a separate slot of time in an asynchronous connection.

A few systems used connection-oriented exchange of message, which became obsolete with the new systems and standards (for control purposes).

Proprietary systems make increasing use of routine broadcast service, sometimes called multicast messaging, or global data. The advantages of routine broadcast service for control purposes are shown in Section 5 see [B29] and [B36] . Requests for routine broadcast data links have become preferred by users, manufacturers, and standards writers (see Section 6.5 see also [B38] , [B39] , [B41]).

Protocol unit or message frame format, which is sometimes improperly called “protocol,” has been specific to each proprietary system. Some systems have emphasized the integrity of the received message at the expense of response time, others were more concerned with a short format and a short response time [B35] , [B9] . The tendency has been to use a frame format of the HDLC type see [B35] with double address, variable information field length, and 16-bit cyclic redundancy check (CRC) field. There were as many signaling methods as there were systems [B52] .

The recent signaling methods are self-clocking (that means that the synchronization of transmitter and listener does not need a special and separate clock signal), and have a Hamming distance of 4 [B29] . The baseband Manchester and carrierband modulation are the most common signaling methods now. Currently, the bit rate ranges between 1 and 10 Mbps.

Copyright © 1991 IEEE All Rights Reserved

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS Not for Resale

6.4.4 Medium Access Control (MAC)

Medium access control methods were described in general terms in Section 5 The following discussion refers to proprietary MACs used by marketable systems and the tendencies in this field.

With the impact of the OSI model on networking techniques, new MACs surfaced, with a common attribute, namely, no centralized facility. All data stations have an equal right to access the medium, as long as the protocol rules are met. MACs derived from the OSI model are store and forward, token passing, and CSMA/CD. They all have merits and demerits, and are used by one or another manufacturer.

Other systems use a central address transmitter, which permits all stations in turn, to access the bus (cyclic reporting). All central facilities are dual or triple redundant, which makes for high dependability.

For example, bus arbitrator facilities as masters of the communications medium have had a remarkable comeback (see 6.5 and [B40]). The bus arbitrator is based on a simple protocol (MIL 1553B). It allows all stations to transmit, in turn, directly to the plurality of interested addresses, contrary to HDLC/SDLC protocols, where the master establishes a connection-oriented session only between itself and one of the slaves. The configuration of a centralized bus arbitrator network is not a star, but rather a bus or ring, which has several advantages over a star configuration.

The CSMA/CD, an alternative of MAC methods known under the name of “contention,” is also used for control purposes. While this method has a lot of advantages, such as speed and simplicity, it has disadvantages when used for control networks. Its indeterministic characteristic (see Section 5) has been lessened through additional measures introduced to the MAC of the CSMA/CD protocol.

Token passing (either in a bus or ring topology) has its own advantages and disadvantages, as shown in 6.3.2.1 see also [B36] .

A specific suggestion for MAC is premature, because of the controversy that exists in this field. For example, new developments adopted token bus MAC [B34] , [B38] ; others (especially for field buses) adopted the address transmitter (see 6.5).

6.4.5 Impact of IEEE 802 Standards on Marketable Control Networks [B28]

In 1980, IEEE 802 began to develop a family of standards for networking computer systems. Several (more than ten) local area network (LAN) standards for the general purpose of distributed data processing have been approved. According to IEEE 802 scope and purpose, these standards could be used also in light industrial environments.

The merit of IEEE 802 standards consists of demonstrating the feasibility of high speed LANs, their advantages as compared with telephone line network, and the general organization of LAN's protocol.

Some distributed control manufacturers adopted either the CSMA/CD (802.3 or Ethernet, which are very similar) or the token bus (802.4) for their control network, but all of them made improvements to respond to industrial applications.

IEEE 802.4 standards (broadband and carrierband) were adopted by MAP specifications, (see 6.5.2).

IEEE 802 standards begin with 802.1, which includes network management functions (see Section 5).

Data-link services, specified by 802.2, are limited to connectionless with no acknowledgment and connection-oriented message sessions. Both of them are inconvenient for control purposes, the first because of safety reasons, the second for being too time-consuming. More link services were added recently, such as Type 3 LLC with acknowledge service.

The disadvantages of broadband media, specified by 802.4 standards, are shown in 6.5.2 from the point of view of power plant control applications.

Copyright © 1991 IEEE All Rights Reserved

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS Not for Resale

6.5 Hierarchical Network Architectures and the Field Bus

The need to integrate the control systems, mounted on the plant floor, with plant and corporate management computers (computer integrated manufacturing, [CIM]), a tendency especially emphasized by the parts manufacturing industry, has brought about many computer network hierarchies. They try to link together as many functions as possible through a reduced number of networks. The network architecture has become a hierarchy of networks connected by gateways and bridges.

Each application requires a definition of the functions and proper specifications of each network. A selection of the networks' links is required to meet the type of industry, and the specific requirements of corporate management.

We can define the following networks that may be connected:

1) The diagnostics network, a network that links non-destructive test instruments with the operators and maintenance workshop, mentioned in 1.2.1.3 as plant diagnostics task.
2) The field network, which services the field instruments and the I/O devices.
3) The intermediate control network, which services the local and group controls.
4) The main plant control network, which services the central plant facilities at the unit level.
5) An office automation network, which services plant and corporate management functions.
6) A corporate management computer network, which services the management information system (MIS).

Such a hierarchy may be costly, bulky, and difficult to maintain and reconfigure. It should be designed and tailored for each specific application. A practical hierarchy is needed.

6.5.1 Proprietary Network Hierarchies

Some manufacturers offer a subnetwork (bus) for each segment (island, group) of the plant. The subnetworks are linked to a main plant control network.

The response time of such a hierarchy could be rather long, due to the utilization of gateways. The complexity of maintenance, repair, and network management is high.

Some recently developed proprietary network hierarchies emulate to some extent the manufacturing automation protocol (MAP), with improvements.

6.5.2 Manufacturing Automation Protocol (MAP), Version 3.0

MAP was initiated by General Motors for their own needs. The intent of MAP was to select a set of standards for a factory LAN and specify the interfaces between multivendor products in order to support communications among big computers and control devices specific to the discrete parts manufacturing industry.

This corresponds to the goals of any CIM (computer integrated manufacturing) tentative implementation.

MAP's Version 3.0 officially adopts an enhanced performance architecture (EPA) with a main network (the backbone) and subnetworks (miniMAP) or “control segments.”

The backbone protocol has chosen IEEE 802.4 broadband, while the subnetwork protocol has chosen 802.4 carrierband, in order to avoid gateways between the two networks.

MAP's Version 3.0 backbone presents some disadvantages from the viewpoint of a power plant control network's dependability [B30] . multichannel media should be avoided in order to meet the fault containment required. MAP broadband is not redundant. A control network for power plants should be redundant. MAP backbone has many single points of system failure, such as headends and complicated frequency agile taps.

Copyright © 1991 IEEE All Rights Reserved

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS Not for Resale

MAP's network architecture including the backbone has a transaction time in the range of seconds, while the response time of a power plant control system should be restricted to a range of milliseconds.

The big advantages of MAP's backbone are:

1) The length of the broadband coaxial cable stretches over 10 km distance.
2) The multivendor supply using standard OSI products, if interpretability requirements could be met.

Some more details on MAP are in [B30] and [B39] .

6.5.3 Derived Network Hierarchies from MAP's Architecture and Protocol

Some manufacturers have recently developed “open” systems that meet acceptable specifications of MAP. They accepted the 802.4 carrierband (MAP’s control subnetwork) as the main plant control network. The backbone with seven-layer stations and broadband network implementation is not yet in use.

One source [B34] offers 802.4 either carrierband or broadband as the main plant control network, and added field buses to its nodes. It has been announced that a link and a MAP backbone will not be developed until MAP specifications become stable and definite.

Another vendor has adopted the 802.4 carrierband for the main plant control network, but added a kind of routine broadcast among the data link services that is a proprietary feature. No intention to develop a MAP backbone is mentioned see [B38] .

6.5.4 Field Buses

The field bus is a serial bit, bidirectional communications link between intelligent sensors/actuators, control devices, data processing units, etc., that replaces hardwired signaling techniques such as continuous and ON/OFF. Their main purpose is to ensure more information flow (and consequently, consistency) in a more reliable way with more accuracy and at less expense.

Advantages of a field bus can be summarized as follows:

1) Wiring-cost savings
2) Improved data validity through self-diagnostics messages
3) Improved accuracy and linearization
4) Elimination of the scaling at the transmitter's output
5) System access to the full sensor range, not a scaled subset
6) Additional identification information available
7) Automated calibration records
8) Up- and down-loading of transmitter configurations
9) Easier installation, commissioning, and maintenance
10) Reduced instrument model spare units

6.5.4.1 Field Bus Standardization Efforts

There are several standards organizations drafting field bus standards. Among them are the IEC (International Electrotechnical Commission) SC65/WG6, the ISA SP50, the French FIP, Eureka (European Common Market), PROFIBUS (German), and NEMA (National Electrical Manufacturers Association).

The field bus standards mentioned in the following paragraphs are under development at the time this Guide was written. Changes in these standards should be expected until they become official.

Copyright © 1991 IEEE All Rights Reserved

--`,,`,,`-`-`,,`,,`,`,,`---

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS Not for Resale

6.5.4.2 Factory Instrument Protocol (FIP)

A technically advanced open field bus is a FIP. This draft standard has been worked out by many French and Italian companies, research institutes, and American control manufacturers located in Europe.

The guidelines of this bus are:

1) Information consistency for all data available on the bus
2) Optimization for cyclic acquired data
3) Guaranteed cycle duration and access time
4) Non-cyclic data exchange in a dedicated cycle slot
5) MAP and PROWAY transparent operability
6) Dynamic configuration (fault tolerance, hot repair, change of station location and number during regular service)
7) Synchronous transmission of data acquisition messages in less than 10 ms.
8) Routine broadcast with identifier transmitter, transferable among several stations
9) Bus topology (see Fig 11).

Figure 11 shows, on the left side, a two-level architecture with MAP and FIP. On the right side of the same figure, a triple level architecture is shown, with MAP, PROWAY, and FIP.

6.5.4.3 ISA SP50 Field Buses

ISA SP50 Field Bus is more concerned about the current architecture of instrument hardwiring. SP50 designates one area of application, called H1, dedicated to replace the 4–20 mA signaling and a second area of application called H2, for high performance systems. H1 is a star configuration that maintains the principle of single loop integrity. H2 is presumed to have a star topology from instruments to a junction box and further on from the junction box to the control room—a multidrop bus configuration.

Long debates about the two alternative data link services, namely, the “token-passing” and the “changing master” protocols, have resulted in the adoption of the changing master protocol. This latter protocol corresponds to item 8 of the FIP protocol (see 6.5.4.2); that is, routine broadcast with identifier transmitter (master) transferable among all or several stations.

6.5.5 Non-OSI Network Architecture

As was mentioned in 6.4, some manufacturers link several control network segments through a large and central computer facility, in order to integrate the entire plant control. Such a network architecture is illustrated by Fig 12.

A superimposed network over a field bus takes about 50 ms to service the group and the unit levels (see Section 4). Another solution consists of using more developed field buses to service the field instruments, the local control, and group levels, while the highest level (unit) that integrates all the field buses and process superior programs consisting of a fault tolerant multiprocessor center. This solution avoids the use of any gateway or bridge. The total response time of the network is potentially faster, since the multiprocessor capacity may proceed in 100 μs or less instead of many tens of milliseconds. High-level programs and supervision through CRTs may proceed faster see [B31] .

The total cost of such a system is potentially less than a regular network hierarchy because less communication equipment is necessary.

Copyright © 1991 IEEE All Rights Reserved

--`,,`-`-`,,`,,`,`,,`---
Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS Not for Resale

7. Data Acquisition and Monitoring

7.1 Introduction

This section of the application guide is concerned with the human or man/machine interfaces (MMIs) of the distributed control system, and provides some guidelines on human factors engineering. Human factors engineering is concerned with designing machines with environments so that they match human capacities and limitations. The reader is directed to [B69] –[B73] , [B81] , and [B82] for these details.

Section 7 encourages the use of artificial intelligence (AI) expert systems to be included in the data acquisition monitoring system. The value of an AI expert system increases when the risk of damage or injury is great. The AI expert system is able to sort through a great deal of process information (such as alarms), deduce the cause of an "event" and determine one or more possible solutions. Although an AI expert system may or may not take any direct control action, it provides valuable information to help reduce risk. The reader is directed to [B53] and [B54] for these details.

The data acquisition and monitoring functions provide operational and maintenance personnel with the information and means to effectively operate power plant processes. The data acquisition and preprocessing functions take place at or near the I/O equipment of the distributed control system. This I/O equipment can be located centrally or distributed geographically throughout the power plant. Other data acquisition functions internal to the distributed control system are as follows: reporting, monitoring, operating, diagnosing, plant performance evaluation, optimization, and processing. These functions are performed by the microelectronics and software programs located throughout the distributed control system.

7.2 Man/Process, Man/System Interfaces

There are three subsections in 7.2 of the application guide. Section 7.2.1 is devoted to the man/process interfaces and related functions, 7.2.2 to the man/system interfaces and related functions, and 7.2.3 to the CRT display design. Figure 13 illustrates these interfaces as follows:

a) The man/process (virtual) interface serves as the primary communications link between the operating personnel and the power plant processes. This allows them to monitor, operate, and optimize those processes.
b) The man/system physical interface consists of man I/O devices, buses, processors, power supplies, electronic modules, etc.
c) The system/process interface is a physical interface where the plant processes and mechanical equipment as sensed by pressure, temperature, flow, instrumentation level, etc., are input into the distributed control system for data processing.
d) The man/system diagnosis interface is a combination of the self-diagnostic functions and the system communication testing. This provides plant personnel the ability to readily isolate a failure or potential failure in the control system.

Copyright © 1991 IEEE All Rights Reserved

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS Not for Resale

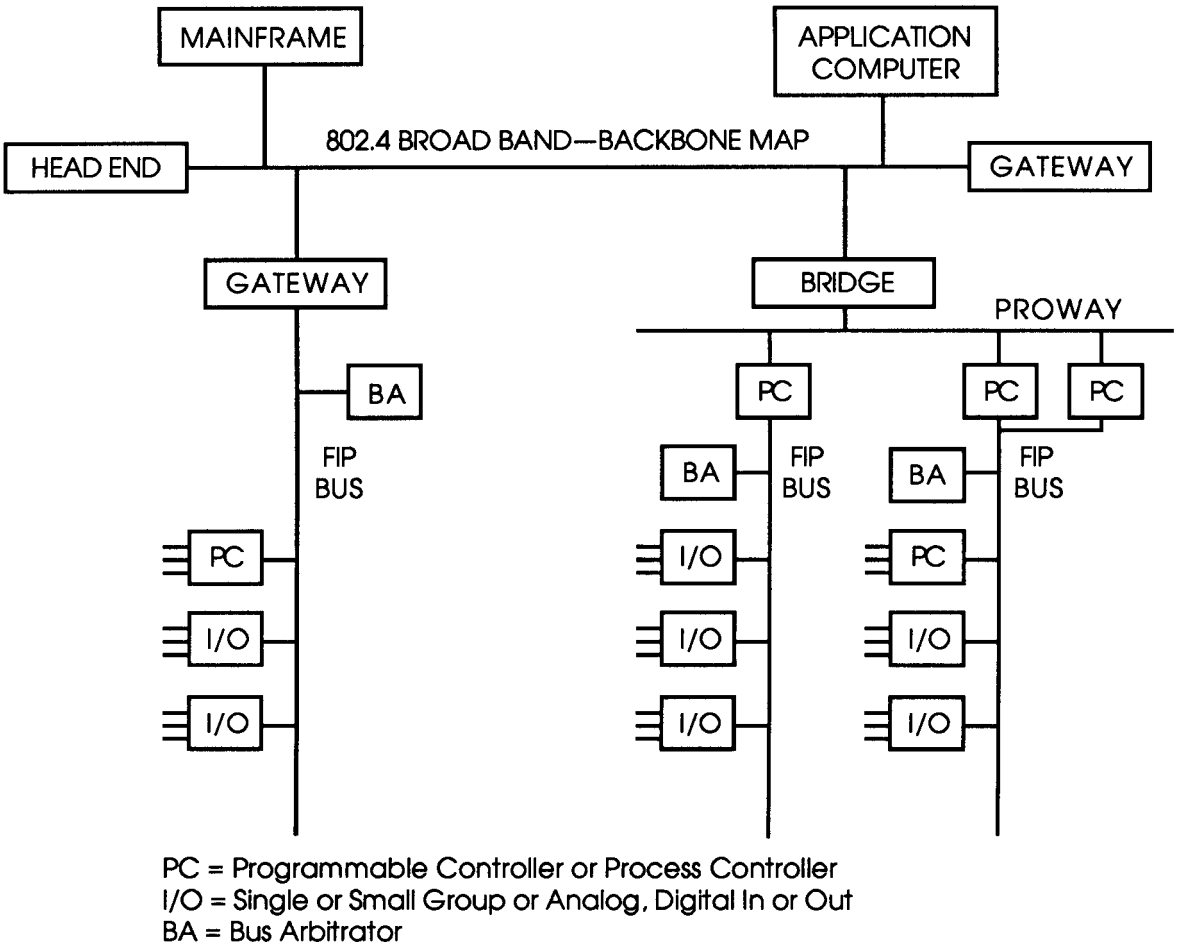


Figure 11—System with MAP/PROWAY and FIP Bus

Copyright © 1991 IEEE All Rights Reserved

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS
Not for Resale

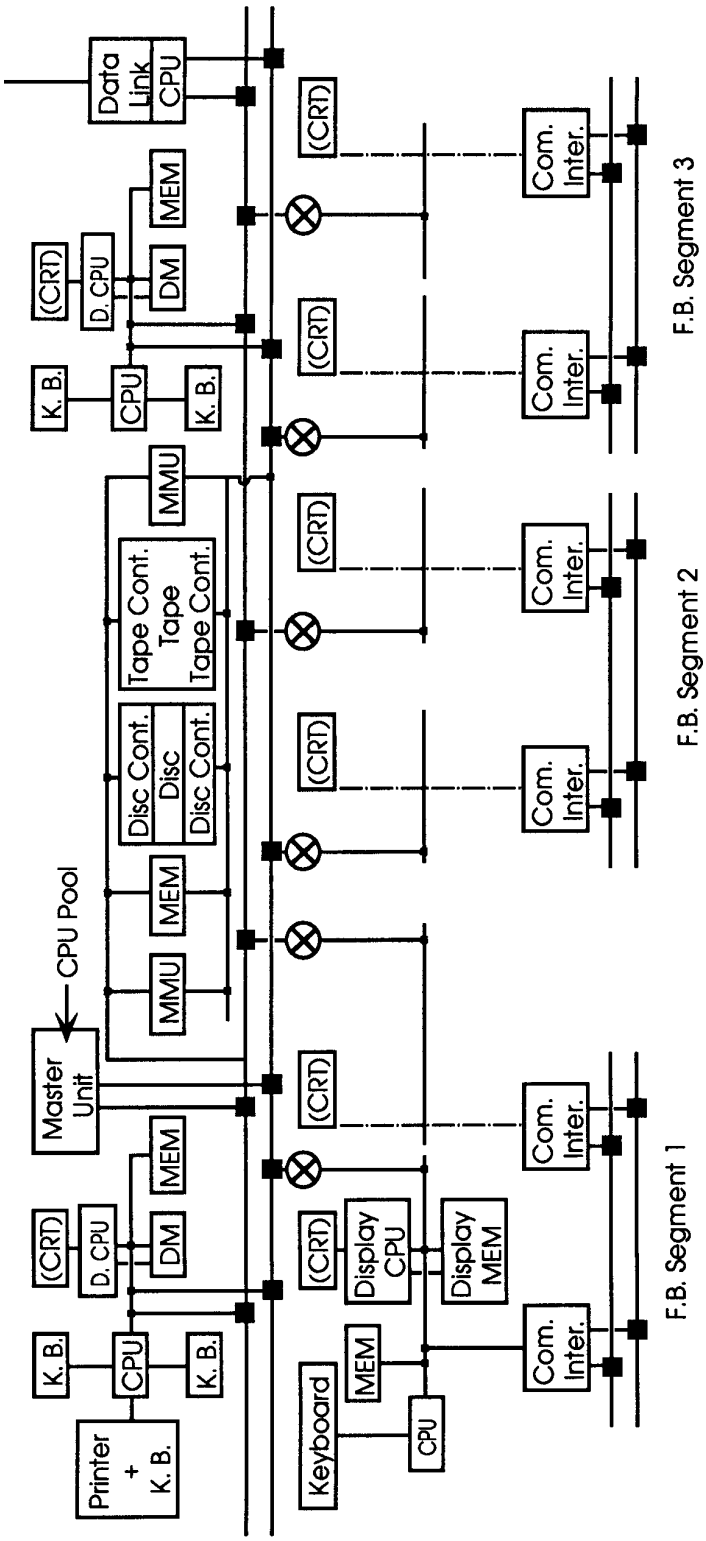


Figure 12—Multiprocessor Level 3

Copyright © 1991 IEEE All Rights Reserved

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS
Not for Resale

7.2.1 Man/Process Interfaces and Related Functions

Man/process interface functions are operating, monitoring, reporting, optimization, processing, and data acquisition, and preprocessing. Figure 14 shows how data flows between the different functional portions of the distributed control system for the man/process interfaces and related functions.

7.2.2 Man/System Interfaces and Related Functions

Man/system interface functions are fault detection, reporting, system- and self-diagnosis, and testing. The man/system interfaces are directly linked to the repair and maintenance facilities. The repair of some faults should be guided by an expert system, based on the system's diagnosis capability. Figure 15 shows the data flow concerning the man/system interface. If a problem occurs within the system, e.g., at a data station, this data flows through the communications network to monitoring, to reporting, to data manipulation, and then to the system operator. Refer to Sections 5 and 6 for further details on how the medium is supervised and reports problems.

The system should undergo a systematic test and self-diagnosis. Beginning with the I/O system, all modules and components should be provided with self-diagnosis capability. The field instrumentation should be tested directly or by simulating circuits. Some redundant or fault tolerant active components, grouped by pairs, or by an assembly of three units, can undergo a mutual diagnosis on top of the self-diagnosis. Some units can be used as checkers for other groups of modules.

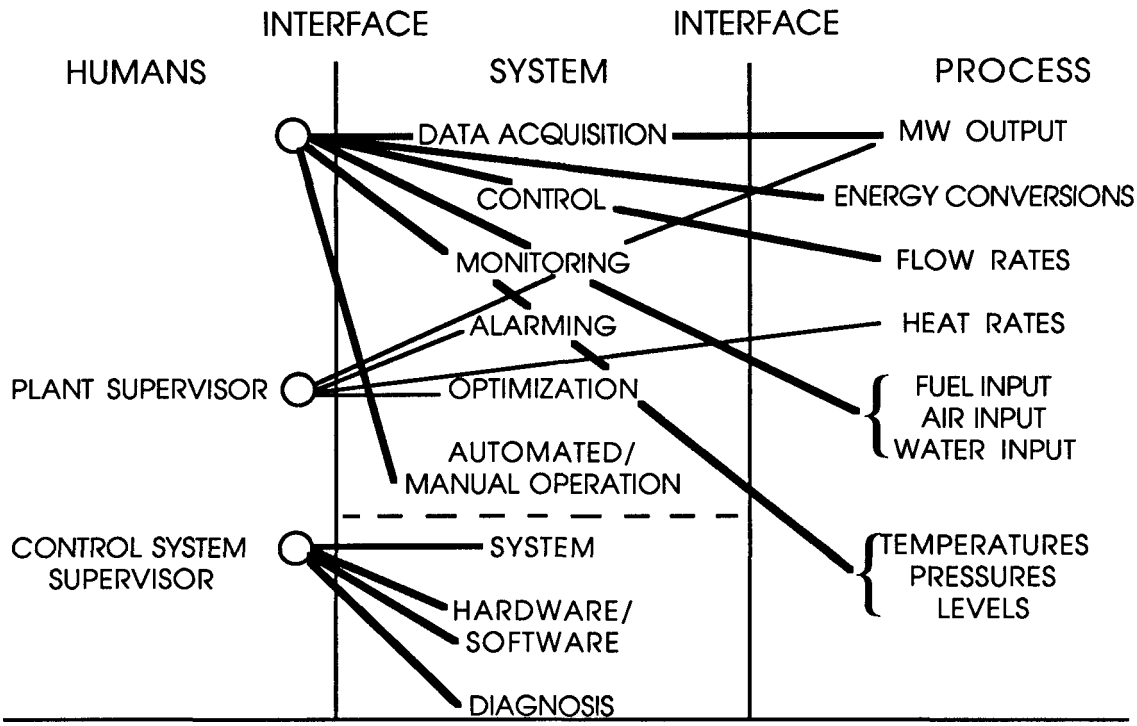


Figure 13—Man/Process Interface, Man/System Interfaces

Copyright © 1991 IEEE All Rights Reserved

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS
Not for Resale

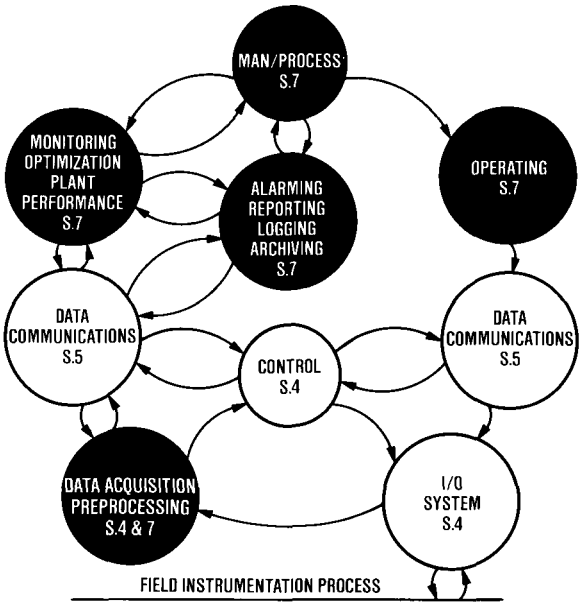


Figure 14—Semantic Network I, Man/Process Interfaces

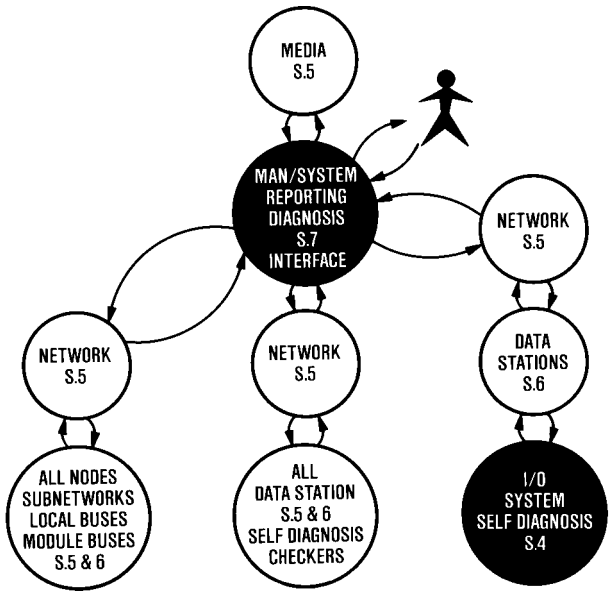


Figure 15—Semantic Network II, Man/System Interfaces

7.2.3 CRT Display Design

7.2.3.1 CRT Display Techniques

CRT display techniques are almost unlimited. Because of this, certain guidelines are given in this section and 7.2.3.2 to ensure optimum information display. The reader is directed to references [B43] –[B45] , [B47] , [B48] , [B51] , [B57] , [B59] , and [B68] for further details. Formats for displaying the information should be considered, should be unambiguous, and should be easily assimilated. Some of the more important are as follows:

Copyright © 1991 IEEE All Rights Reserved

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS Not for Resale

a) The approach to the design of a CRT display should start with the user, and design the display for the user. The man/machine consoles should be optimized for each user; i.e., manager, engineers, maintenance personnel, and operators. The user should have the ability to configure graphics, on-line, while the process is running.
b) The designer is cautioned that a CRT is only a “limited” window view of the total process and that the CRT displays should be designed cautiously and evaluated with actual operator input and feedback during the design process. Therefore, the number of CRTs available to the operators to view the process can become critical at certain times, such as unit startups and response to trip conditions. Careful consideration should be given to having sufficient numbers of CRTs available for use during these situations.
c) The operator interface should be the same for all control and monitoring functions. The location, layout, and orientation of data and objects on CRT displays must be consistent and logical such that the operator will instinctively know where on a CRT display to find the needed information.
d) Picture content should be structured to contain only vital and essential information. The most important information should be the data and not the precise physical layout of the plant equipment.
e) Data required for the evaluation of operating status of the plant systems should always be complete and provided quickly to the operator.
f) The CRTs should be positioned and allocated according to the control philosophy of the power plant. As a minimum, it is suggested that at least 4 CRTs and two keyboards be provided. These should be for a dedicated alarm screen, two operator screens, and a utility screen. It also allows for the loss of up to one half the screens while maintaining a minimum of at least two screens. (See item “b” above.)
g) Data relevant for a plant system must be selected to permit evaluation of whether or not the respective system is functioning correctly.
h) Standardized rules regarding color usage, operating status, picture area arrangement, data display, number of predirect points, graphic programming, and symbols are to be observed for the picture layout.
i) Human factor engineering (ergonomics) and anthropometric requirements including imagery techniques, resolution capacity of the eye, recognition of characters, flashing functions, and dimensional adaptations should be considered.
j) It is suggested that any CRT screens designed to be viewed while moving around the control room should be at least 25 inches in size, while sit-down operator consoles can be 19 inches.
k) All process graphics should be linked in the same order as the process itself, so that the operator may easily proceed forward or backward through the graphic displays with single keystrokes.
l) Display hierarchy techniques should be incorporated to enable an operator to proceed from overviews to group/subsystem displays and back to obtain process detail.
m) Avoid unnecessary interface actions, such as too many buttons or keystrokes, to move through displays. The design should be such that minimum actions are necessary, except in the case where security is necessary to prevent unwanted actions. A release or verification technique should be required where inadvertent initiation could be detrimental.

7.2.3.2 Guidelines for Designing CRT Displays

7.2.3.2.1 Display Orientation/Layout

Some considerations are:

a) Cognitive Fidelity: CRT displays provide process information to operators. It is important that this information match the operators’ cognitive expectations that have formed during training and hands-on experience. Example: show boiler temperature as 950 F (not in centigrade and without degree sign).
b) Stimulus Correlation: CRT displays also provide visual stimulus (pictures) to operators. It is important that CRT pictures match the operators’ mental pictures of plant equipment and systems, providing stimulus correlation between CRTs and the actual plant; e.g., show condensers below turbines and with condenser level in blue to match water.
c) Display Heading: To allow for grouping of similar or related graphics in a menu, the heading of the graphic should start with the main system involved followed by a description of the function; for example, coal mill operation and turbine vibration measurement.

Copyright © 1991 IEEE All Rights Reserved

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS Not for Resale

d) Information Flow: The flow should be consistent for all displays. It should be from left to right and from the top down. Visual entry into a display should be from the upper left and exit to the right.
e) Position: Where possible, the position of equipment on the pictorial should be in the same relationship to each other as in the plant. Equipment that is at higher levels should be at the top of the pictorial and equipment at lower levels should be at the bottom.
f) Natural Movement: Displays showing changes in quantity should have pictorial and/or alphanumeric movement in the display consistent with the movement of the process; for example, if water level rises in a vessel, the level indication should go up.
g) Quadrant Preference: The eye scans in a predictable manner. Plan tabular and text presentations or information so that the most important is in the quadrants in this priority:
    1) Upper Right
    2) Upper Left
    3) Lower Left
    4) Lower Right

NOTE — This does not apply to pictorial presentations where stimulus correlation is more important.

7.2.3.2.2 Information Presentation

Some important considerations are:

a) Word Orientation: Words should be horizontal when used in a pictorial, text, or tabular format.
b) Symbol Size: At a normal viewing distance of 28 inches, complex symbols should have a height of approximately 0.16 inches. This is equivalent to a visual angle of the symbol subtending an arc of 20 minutes at the required viewing distance.
c) Alphanumeric Character Size: At a normal viewing distance of 28 inches, the height of alphanumeric characters should be approximately 0.1 inches. This is equivalent to a visual angle of 12 minutes of arc at the required viewing distance.
d) Legibility: All alphanumeric information on displays and text should be readable by the operator from a 28 inches distance as a minimum.
e) Density of Graphics: Overall density is expressed as the percentage of the overall character spaces available that are used. Moderate density is most effective and low and high densities are less effective. Moderate density is about 25%. High density displays should be field tested.
f) Text Word Length: Suggest six characters or less, but should have 12 character capability if required.
g) Numeric Word Length: Suggest four characters or less.
h) Number: Numeric strings represent values being measured, such as temperature or pressure. Strings should be broken with spaces every 5th line (or column). Do not show values to too many decimal points, such as a temperature of 100.23456787. For example, for values greater than 100, use no decimal places; for values between 10 and 100, depends on the process parameters; for values less than 10 use one decimal place; and for values of less than 1, use two decimal places.
i) Text: Text strings should be kept to a minimum, and heavy reliance made on graphic pictures. Text should be used to help orient the operator or to explain conditions not easily shown in pictorial format. In general, capital letters are suggested. Use a font that is easily read on the CRT. Adequately space letters, words, and lines of text. Be sure words are clear, concise, and unambiguous.
j) Symbols: Symbols should be uniform in construction for the same type of device. For example, all pumps should use the same general symbol. Orientation of symbols to right or left, up or down, may be necessary, but should be limited if possible. In addition, dynamic symbols should be clearly identified from static symbols through the use of both color and text to minimize color recognition problems. Symbols should be designed to reflect the process rather than show physical construction when possible. Figures such as valves or pumps may be active or passive.
k) Color: Used primarily to show changes in status and with other methods of presenting information. It is suggested that the use of color be limited to approximately eight colors foreground or background per display. This includes the use of reverse video. Rules for the use of color should be uniform from display to display;

Copyright © 1991 IEEE All Rights Reserved

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS Not for Resale

e.g., red may indicate an open valve or running motor, but should not also be used to indicate a static pipe for hot reheat, as this could confuse the operator.

l) Blink: Flash used to attract attention. A single blink rate between 2 and 5 Hz is suggested.
m) Auditory: Sound should be used to call the operator's attention to events where action is required. Care should be made to regulate the sound level to medium intensity.
n) Upper and Lower Case: Use all uppercase letters unless the CRT resolution is 640 by 480 pixels or more.
o) Brightness: CRT symbol brightness should be used to help draw the operator's attention to the most important information on the screen. The use of brightness to differentiate devices (such as condensers versus deaerators) is not suggested. Avoid extreme brightness differences between the CRT and the room, and on the CRT screen. Contrast ratios on the CRT screen between 3:1 and 15:1 are preferred.
p) Size: Character size should be considered when designing the displays; e.g., an alarm screen that needs to be readable at some distance should use larger characters than characters on a P & ID pictorial used to show feedpump identification.

7.2.3.2.3 Color Code

When selecting colors for use in displays, the following should be kept in mind:

1) Colors in general:
   a) Color should be used to enhance the presentation of information.
   b) The color should be selected to fit the function.
   c) Color should be used as a form of redundant coding; for example, used along with other methods such as flashing or shape coding.
   d) The mental set of the operator should be considered when colors are being assigned to functions. For power plants, the color RED is used to indicate energized and this should continue: likewise, GREEN is utilized to represent a de-energized state.
2) Number: The number of colors used should be restricted to not more than eight including black for background. The use of "half tones" should be limited to 30 for special effects such as animation, 3D effects, etc.
3) Function: Colors should be used to show process and condition of equipment or of lines, rather than classes of equipment.
4) Loss of Effectiveness: Color coding may be less effective on the periphery of the visual field and for operators over the age of 35 years.
5) Color Blindness: Color blindness affects about 6% of the population. This should be kept in mind so that colors are not the only means of presenting information, particularly where the information is safety-related.

7.2.3.2.4 Symbol Conventions

The following are some things to consider when planning the layout of graphic displays:

1) A number of common symbols are used with CRT displays and in particular for use with pictorial displays. These symbols should be based on the piping and instrumentation drawings utilized in the control room by the operators.
2) Valves: The symbol for a valve may be vertical or in-line. It may show an air-, hydraulic-, or a motor-operated actuator. The valve may be static, but it may also be dynamic where the condition is shown by the valve changing color or the valve symbol including a colored lamp.
3) Status: Valves should show status by colors and/or text:
   a) Open
   b) Closed
   c) Failure (valve command not executed or changed state without command)
   d) Valve in travel
4) Signal status should also be denoted by color and/or text:
   a) Good value
   b) Alarm

Copyright © 1991 IEEE All Rights Reserved

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS Not for Resale

c) Bad value
d) Inserted value

5) Pumps: The symbol for a pump is generally in line, although the throat may be pointed to the left or the right. The pump may be static but may also be dynamic, with the condition of the pump shown by the color of the symbol.
Pump status should be indicated by colors and/or text:
a) Energized, in operation
b) Not energized, but ready for operation
c) Tripped
d) Tripped, not acknowledged
e) Failure (command not executed)
f) Not available, out of service
6) Dampers: The damper symbol may be one, two, or three diagonal lines, or it may be a number of diagonal lines with a center space to show the status to the damper. Dampers may be shown static or dynamic.Damper and signal status should be indicated, as for valves.
7) Electrical Breakers: Electrical breaker status should differentiate among open, closed, normal, and tripped conditions.
8) Line Codes: The process flow diagrams representing piping or electrical lines should be coded dynamically to show the following conditions:
a) A line has pressure, flow, or energy.
b) A line has no pressure, flow, or energy.
c) A trip or failure in a line or the associated equipment.
d) The distributed control system is reading a field device with a suspected failed input.

7.2.3.2.5 Static Displays

These are the static portions of display; i.e., those that do not change with process conditions. Color conventions should be established to distinguish among the various lines and symbols.

7.2.3.2.6 Abbreviations

Abbreviations and acronyms should be consistently utilized on the panel legends and the annunciator alarms. It may not always be practical or desirable to have these exactly the same, and a separate list of acceptable abbreviations and acronyms for use in the CRT displays should be kept. Typical display abbreviations are short, often three to five letters. Do not include a period; periods provoke unnecessary attention.

7.2.3.2.7 Control Room Lighting

When implementing the CRT design process, one must consider the overall ambient lighting effects. One must consider horizontal and vertical surfaces near the CRT display. If possible, the colors selected for the various CRT displays should be evaluated under the actual control room lighting conditions.

7.2.3.3 Performance Criteria of CRT Displays

7.2.3.3.1 Speed

There are three speeds that directly affect CRT usability. These are: (1) system indication to the operator that a requested action is underway (it saw the key push), (2) the time to complete a new display, including an update of all dynamic information, and (3) the time to indicate the completion of an action (minus the process delay). System indication cannot be too fast and should be less than one second. A new display should be under two seconds. The update of dynamic analog information on a display currently being viewed (not a new display) should not be more rapid than every two seconds. State changes should update as fast as possible.

Copyright © 1991 IEEE All Rights Reserved

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS Not for Resale

Upon the operator's request, an image should begin to change in less than one second. After that, the changing rate of the entire picture should be higher than the operator's perception power. The time consumed by transmitting, receiving messages, and data processing must be included in evaluation of this image response time.

The response time of a CRT monitor can be split into several phases, such as data processing, data communication through all involved serial and parallel data paths, write/read memories, serializing of bits to the color monitor, scanning, etc. Except for data processing and data communications, all other phases can be included in the data manipulation phase.

7.2.3.3.2 Resolution

Resolution is measured in several ways, which can be confusing for users. The usual way to specify resolution is the pixel number. High resolution is around 1500×1200 pixels, used especially for complex graphics. Medium resolution, satisfying most plant monitoring displays, is around 640×480 pixels. Switching between these two resolutions is possible and permits different kinds of images to be displayed with the most appropriate resolution for that display.

Resolution is also defined in pitch, the diameter of red-green-blue (RGB) dot trios. A medium resolution pitch is 0.31 mm, which is acceptable. A high resolution pitch is 0.2 mm.

7.2.3.3.3 Quality of CRT Monitors

The image should be flicker-, glare-, rainbow-, and reflection-free. The CRT terminal should have a ruggedness for industrial applications, with longer life and increased resistance to dust, oil, and moisture.

7.2.3.3.4 Process Variable Trend Requirements

Trends of process variables should be presented in real time with one to ten minute resolution. Historical trends should have a span from five minutes to several days, with decreasing resolution.

7.2.3.3.5 Animation

Changes can be emphasized by motion to aid in clarifying the data as presented to the operator. Flow through pipes, level in tanks, etc., can use convolution techniques to show motion.

7.2.3.4 Imagery Techniques (Imagineering)

7.2.3.4.1 Manual Data Manipulation

Imagery techniques refer to the science and art of automatically presenting information by images (automated data manipulation). The means by which the operator can request information and implement commands through the distributed control system constitute manual data manipulation.

For power plant operation, acceptable means of image manipulation are hardware and software labeled keys and touches. As pointing devices, digitizing tablets, mouse, joysticks, trackballs, and lightpens should be discouraged for human factor engineering (ergonomic) reasons. An auxiliary touch-screen, besides a main (touch-free) screen, presents advantages. The main screen is kept clear, smudge-free, and clutter-free. The touchpad can be installed to meet ergonomic conditions. The touchpad will leave the possibility for the operator to continuously follow the image motion, while his fingers will manipulate the image, as is the case in driving a car.

The use of voice for data manipulations will be available in the near future. Sound will enlarge into a new dimension, as a parallel means for man/machine interaction. This will accelerate data manipulation. The ergonomics effects of the parallel use of vision and sound are not yet known.

Copyright © 1991 IEEE All Rights Reserved

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS Not for Resale

7.2.3.4.2 Use of Imagery Techniques

Features of imagery techniques consist of coloring, graphics, 3-D, windowing, zooming, scaling, panning, scrolling, shading, clipping, flashing, and animation. These features should be used in a productive way.

a) Three-dimensional representations should be used with mechanical equipment and semantic networks, where the third dimension will add to the understanding of the image message.
b) Windowing describes the possibility to partition the screen, and to separately display each partition or window enlarged to the full screen size. Each window can be separately scrolled, panned, or modified without affecting the neighboring windows.
c) Zooming or telescoping is a means by which the image goes in-depth to a targeted end to show the details of the selected spot. This is done by motion pictures. As the migration through the images progresses, more details are added to the pictures.
d) Scaling is the capability of images to shrink or enlarge, at the operator's or machine's command.
e) Panning is the ability to locally rotate an image to see other aspects of a picture.
f) Scrolling is the capability to smoothly move the picture, vertically and horizontally, in order to see adjacent portions that have not entered the screen. It is useful especially with drawings.
g) Shading provides the possibility to dynamically change color shades for emphasizing a process evolution or state change.
h) Clipping is a feature of imagery techniques that permits the operator to rapidly scan through a set of pictures in order to select one that is of interest. Also, clipping software routines are used to calculate which part of a graphic object will be displayed on the CRT.
i) Flashing of individual pixels or a group of pixels may be used to emphasize an important message.
j) Animation should be used in relation to dynamics, zooming, and removing of a portion of a figure to reveal details beyond the removed portion and putting back this portion. Also, animation should be used as a pathfinder to targeted spots.
k) A jagged or staircase effect should be avoided by incrementing pixel centers toward an ideal line.
l) In process control oriented pictures, text is always needed for explanations, labels, tags, and so on. Text is also used for presenting selectable menus. A large font selection should be provided with scaling possibilities. By providing shading and color, the text may be enhanced, e.g.; characters on colored background appear to be in the graphic plane, while characters on a black background appear to be in a separate plane, in front of the graphics or vice-versa, depending on shades.

7.3 Reporting Functions

"Reporting" is the general function of making data that was acquired by the system available to other programs within the system, such as "monitoring," and to the operators, through the associated "data manipulation" function. The "reporting" technique has a great impact on the availability of data with respect to time, their correctness, and how input congruency is fulfilled. Reporting performance depends on the I/O system, data acquisition, and data communications functions. The reader is directed to [B46] for details on data acquisition and reporting functions (see also 5.4.1.1.6).

Log information, such as the daily or periodic log, should be considered carefully to ensure compatibility with plant requirements. It is suggested that all logs be "free format" to allow the engineer to customize the format to that required by the plant. In addition, the requirements for redundant printers, printer speeds, and the use of color printers should be reviewed carefully.

Refer to Section 5 for asynchronous burst mode and broadcasting reporting through a medium.

Copyright © 1991 IEEE All Rights Reserved

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS Not for Resale

7.4 Monitoring Function

The monitoring function prepares the data for being reported to the operator and for automatic supervising control. The monitoring function includes alarming, scanning, conversion to engineering units, etc., and similar types of tasks that are related to alerting the operator to abnormal values and logging or calculating information.

7.4.1 Alarm Requirements

The distributed control system database should be the primary plant annunciation source. Visual, audible, and recorded alarms should be provided to alert the operator to off-normal operating conditions and to provide a record of operations events. There are two types of alarms; those about the plant processes as provided by the process system diagnostics, and those about the distributed control system itself as provided by the self-diagnostics. Self-diagnostic alarming should guide the service personnel to quickly identify faulty modules of the distributed control system. Details concerning self and system diagnostics are provided in 7.6. This information should be explicit, to enable the service personnel to exchange a faulty module within an hour at most. How alarms should be selected, presented, categorized, and prioritized has been set down in Alarm, Monitoring, and Reporting System for Fossil Fuel Power Plant Application Guide 676. Also see [B42] , [B49] , [B50] , [B52] , [B55] , and [B56] for further details on alarm prioritizing, reduction, suppression, and management.

Other considerations are as follows:

1) The various displays to accomplish the plant alarming requirements, such as annunciator windows, CRT displays, mimic displays that incorporate alarm lights, and printed displays should all be correlated to ensure that the human factor engineering (ergonomics) requirements have been incorporated.
2) Alarms should be displayed or presented in the order of occurrence. The resolution between alarmed events should be less than one second, although resolution to the millisecond should be provided for sequence-of-events logging. The time tagging of alarms and how they are presented to the operator should not be influenced by the scanning and reporting cycles for the distributed control system. Alarm suppression techniques should be provided to avoid overloading the operator and confusing him during emergency operation.
3) The alarm list or history should be provided on a CRT display. It should consist of all alarm operations, incremental limits, and return-to-normal, with time occurrence, in chronological order. This alarm history should be accessible to the operator with a single keystroke. Provisions should be made to present alarm messages to the operator regardless of the display presently on the screen.
4) Besides CRT display, hard copy data records of alarms as they occur should be provided, as well as a sorted summary or historical record, or as logs for later evaluation.
5) In addition to alarm points, the alarm history should include a record of operator changes to the system, such as selection of auto or manual controller status. This listing may alternately be kept in a separate log of changes to the system; e.g., tuning parameter changes, setpoint changes, points added or removed from scan, etc.
6) It is suggested that the dedicated CRT(s), as required, be provided solely for the alarming functions, although several other methods may also be considered:
    a) Fully dedicated alarm CRT display with switching to another CRT display possible if the dedicated CRT display is out of service. This message page should have other pages available, but the most recent page is shown whenever a new alarm comes in.
    b) Alarm messages (minimum of three) at the bottom of each CRT display with the most current alarms visible.
    c) Alarm messages take priority over other displays and will overlay whatever information is on the screen and will stay on the screen until acknowledged or until the alarm is back within limits.
7) The alarm messages should include this information:
    a) Time: The time of day using a 24-hour clock, with minutes and seconds, should be available. The time information may be available to utilize milliseconds for sequence of events records, but for alarms, resolution to the second is adequate.

Copyright © 1991 IEEE All Rights Reserved

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS Not for Resale

b) Date: The day of the month, month, and year should be available on the screen and on printed output and should be included in any alarm summary.
c) Description: The equipment involved should be described along with the problem.
d) Point Identification: The specific point that is in alarm should be identified.
e) Alarm Status: This should be the condition that caused the alarm. Terms such as HIGH, HIGH-HIGH, LOW, LOW-LOW, ALARM, NORM, OPEN, and DEV should be used.
f) Value: The measured value should be given, or the condition (such as IN, OUT, CLOSED). This value should be dynamic; i.e., continuously updated.
g) Engineering Units: These should be specified (such as PSIA, PSIG, etc.)
h) Limit: The set point or limit value.
i) Warning Signal: When an alarm message comes in or an incremental alarm occurs (HIGH level becomes HIGH-HIGH), a warning to the operator should be triggered; e.g., the time should flash until the alarm is acknowledged. After the alarm clears, that fact should be noted with a separate warning, and upon acknowledgment, the alarm should disappear.
j) Alarm Summary: A separate historical alarm summary should be available and accessible to the operator. This summary should show the alarm messages in the time order that they have been received for the previous shift or longer.

8) An alarm expert system should be included to advise the operator of the correct course of action in much the same way a lead operator would advise a trainee: however, instead of standing at the trainee's shoulder, the expert system's advice appears on the CRT screen.
9) It is suggested that a separate annunciator be included for critical alarms and alarms that must be annunciated upon failure of the distributed control system.

7.5 Operating Functions

The operating function treated in Section 4 receives the operator's commands, translated by the data manipulation function, and implements them through the control function or I/O system. The operating functions are done in real time. Some of these functions include changing of set points, mode of operation, and output state or value of a device.

7.5.1 Data Manipulation Function

The data manipulation function organizes further the presentation of data in accordance with the requirements of the man I/O devices and translates the received digital messages into processed signals for these specific devices. That is, data manipulation is the function that translates a series of ones and zeroes to messages and images in a form understandable to man.

Data manipulation is also the function that receives signals from the man input devices (keys, buttons, touches, voice, etc.) and translates them into digital messages compatible with the system (protocol).

7.6 Diagnosing Functions

Diagnostic and maintenance functions, when performed together, serve to maximize plant availability through minimization of plant outage time; i.e., that time required to identify and repair faulty or failed equipment or to perform normal scheduled maintenance.

Diagnostic functions are used to identify and locate faulty or failed equipment. Maintenance functions are used to identify maintenance requirements, schedule, and provide guidance for all identified plant maintenance activities.

The resulting output of diagnostic functions should be the identification and documentation of faulty or failed control and monitoring equipment or process equipment to the highest level of detail possible. For example, typical levels of detail in fault or failure identification may include identification of faulty thermocouples (specific thermocouples), failed control and monitoring equipment hardware cards (specific cards), or faulty gas turbine combustor (specific

Copyright © 1991 IEEE All Rights Reserved

--`,,`-`-`,,`,,`,`,,`---

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS Not for Resale

combustor). Where they can aid in diagnosing the cause of a failure or help to define alternate courses of action under given fault conditions, expert systems should be employed in conjunction with the diagnostic function.

The resulting output of maintenance functions should be the identification and documentation of plant maintenance status, needs, and procedures consistent with the objective of maximizing plant availability.

Diagnostic functions operate either on-line or off-line. On-line diagnostics run in realtime and therefore provide an identification of a fault or failure essentially at the time of occurrence. Off-line diagnostics are generally those that would require an interruption of the control function, or those that collect data for future evaluation.

Diagnostics are further categorized as self-diagnostics and system diagnostics to differentiate between self-examination of the constituent elements of the control and monitoring system by routines performed by those elements, and examination of other elements of the system, process, or plant by elements of the system.

7.6.1 Self-Diagnostics

Because self-diagnostic monitoring is highly dependent upon the hardware and software architecture of the specific equipment, these functions are usually designed and implemented by the equipment manufacturer. In most cases, it is not possible (nor desirable) for plant personnel to modify or configure the self-diagnostic functions.

7.6.1.1 On-Line Self-Diagnostics

These diagnostics generally use real-time measurements, although certain on-line self-diagnostics may require limited quantities of historical data. Typical self-diagnostic functions may include, but are not limited to, the following:

a) Hardware card voltages over/under range
b) A/D converter offset over range
c) Microprocessor stall (failure)
d) Memory check sums/parity validation
e) Communication failures
f) Processor loading (software) excessive.

Most control and monitoring equipment also employ some form of power-up diagnostics, which are also considered as on-line self-diagnostics since they run at real-time (once) and identify faults/failures at the time the faults/failures occur (at power up).

The results of on-line self-diagnostics are generally some form of hardware-based fault/failure indicator or generation of an alarm or non-alarm type message. More specifically, there are four basic types of outputs from on-line self-diagnostics:

a) Hardware-based fault/failure indicators; e.g., card edge LED indicators.
b) Time tagged non-alarm type operator messages for noncritical faults/failures; e.g., diagnostic message indicating bad memory location on power up.
c) Time tagged alarm messages for critical faults/failures; e.g., loss of A/D converter on an input card.
d) Time tagged alarm messages with preventive measures for critical faults/failures requiring corrective action; e.g., transfer to a redundant element upon failure of its partner.

Certain systems may provide more than the four levels of alarm and non-alarm type messages indicated here, although the additional levels will generally fit into one or more of the basic categories defined.

7.6.1.2 Off-Line Self-Diagnostics

Off-line self-diagnostics are performed on demand by plant maintenance personnel, or are automatically executed at certain periods of plant operation, such as after plant or unit shutdown. Certain off-line self-diagnostics may require

Copyright © 1991 IEEE All Rights Reserved

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS Not for Resale

maintenance personnel supervision. For example, diagnostics to verify digital output actuation requires first that the unit under control be shut down, then that maintenance personnel validate that specific outputs commanded to cycle by the diagnostic functions do actually cycle in the proper fashion.

Typical off-line self-diagnostics may include, but are not limited to, the following diagnostic checks:

a) Control and monitoring equipment I/O hardware validation; e.g., cycle all outputs, etc.
b) Operator interface push-button and lamp tests
c) Communication network equipment tests

7.6.2 System Diagnostics

System diagnostic functions serve to identify faults and/or failures within systems or groups of systems comprised of control and monitoring equipment and associated process equipment. System diagnostic functions reside in control and monitoring equipment at various levels within the system hierarchy.

Identification of faults/failures at the unit level is accomplished primarily using measurements of unit level inputs and outputs and the current operating state of the unit level system. For example, high exhaust temperature during gas turbine startup operation is determined from turbine exhaust thermocouple measurements and knowledge of the current turbine operating state; i.e., turbine startup. Identification of faults or failures or both at the plant level is accomplished primarily using unit level alarm indications and unit level operating conditions. For example, faults/ failures within complete unit level systems such as a boiler system and steam turbine system can be determined by interrogating streams of alarms and operating data from the individual unit level systems. Typically, this function is done by the plant operator, or through the use of specialized routines designed to filter out “unnecessary” alarms and present to the plant operator only the most relevant alarms at the appropriate time.

7.6.2.1 On-line System Diagnostics

On-line system diagnostics are crucial to overall plant protection schemes. Plant and unit protection is accomplished through the identification of deviations of system operation from normal conditions. System diagnostics typically identify two conditions: “alarm” and “trip.” Thus, there are two basic types of outputs from on-line system diagnostics:

1) Alarm messages for faults and failures including, but not limited to, the following:
   a) Sensor failures
   b) Actuator failures
   c) Redundant processor voting mismatch
2) Alarm messages indicating loss of a function or requiring automatic preventive measures (e.g., unit shutdown) for critical faults/failures requiring corrective action (e.g., no answer from a data station on the communications network)
3) Equipment performance diagnostics.

On-line system diagnostics should also include an identification of faults and failures in sensors and actuators, plant equipment, and the process itself. Diagnosis of failures in sensors and actuators, and in connecting wiring, should generally be configured by the manufacturer of the control and monitoring system. Diagnosis of faults and failures in plant equipment and processes will, however, require specific configuration for each plant and therefore must be reconfigurable by the user to permit modification of system diagnostics as plant operating experience increases, or the plant configuration changes.

7.6.2.2 Off-Line System Diagnostics

Off-line system diagnostics identify system faults/failures using primarily historical plant operating data. This identification process is aimed at determining specific sources and characteristics of faults/failures that have occurred or to predict the probability of impending faults/failures. Note that sources of faults/failures may include plant operator induced faults/failures; i.e., operator error. The source of the plant operating data is the distributed control and

 Copyright © 1991 IEEE All Rights Reserved

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS Not for Resale

monitoring equipment. Storage and management of historical plant operating data is usually provided by diagnostic equipment incorporating disk-based memories.

7.6.3 Maintenance Functions

Maintenance functions are responsible for identification of maintenance requirements and providing sufficient guidance for maintenance personnel for the scheduling and implementation of maintenance activities. When used in conjunction with diagnostic functions that identify the occurrences and probable causes of plant faults/failures, maintenance efforts are targeted to maximize plant availability through:

1) Minimization of the mean time to repair identified faults/failures.
2) Prevention of equipment failures through properly scheduled maintenance activities.
3) Maximization of plant operating efficiency through scheduled maintenance activities.

Maintenance functions can benefit significantly from the use of expert systems. Expert systems provide the framework for incorporating methodologies developed by experts in certain fields within an automated environment. In interactive maintenance functions, the expert system can provide “expert” guidance for the maintenance personnel, allowing maintenance needs to be identified and implemented in a timely and consistent fashion. In non-interactive data analysis, the expert system can be used as the mechanism; i.e., algorithm, through which the maintenance needs are identified and implemented.

If expert systems are employed, it is suggested that the expert system rule base; i.e., the set of rules guiding the expert system “condition to conclusion” reasoning process be configurable by plant engineers or maintenance personnel. This is necessary to accommodate the expanding knowledge of plant maintenance personnel as operating experience increases and to accommodate potential plant modification.

7.7 Plant Performance Function

The plant performance calculations function executes performance calculations to measure the performance of the plant equipment. The calculations are done periodically in order to determine equipment efficiency, actual performance of equipment, effect of different operating conditions, and different fuel conditions. Wherever possible, the calculations should be done in accordance with current ASME Performance Test Codes and environmental or similar industry standard procedures. See [B58] for these details.

Plant performance monitoring calculations should be run on a scheduled basis or on demand. Results of calculations should be made available on the communication network for control, alarming, trending, and incorporation into the logs. Measured process parameters should be utilized wherever possible. Manually input constants should be modified only at the engineer’s/programmer’s station unless subject to daily fluctuations.

All data used in performance calculations should be based on concurrent time averages to minimize errors caused by momentary disturbances.

The systems designer is cautioned to the need for sensor accuracy and a careful review of the equations used in the calculations. Also, these calculations are unique to each plant.

7.8 Optimization

The optimization function synthesizes the ideal operating conditions of the plant processes. The results of optimization functions could be checked against the performance calculations. The outputs of the optimization functions can be presented to the operator in the form of graphic displays or actual adjustments to the control functions; e.g., the graphic displays could show worse-reference-better graphs of the deviations in the thermal consumption of the turbine/generator system. Control adjustments based on the results of stoichiometry calculations could change set points on the controllers to provide an optimum ratio of one parameter to another to save on the operating and equipment costs.

Copyright © 1991 IEEE All Rights Reserved

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS Not for Resale

7.9 Processing

The database is processed and stored throughout the distributed control system. An important point is that the computer processing of functions internal to the distributed control system, such as alarming, monitoring, and data acquisition, should be transparent to the operating personnel. The operating personnel are more concerned with the results of these functions and how well they are presented rather than how these functions are accomplished. However, when there is a malfunction within the distributed control system, it should be presented to the operating and maintenance personnel in a clear and concise manner. The presentation should avoid confusing a control system problem with a plant operation problem.

7.9.1 Database

The distributed control system should have a distributed and a fault tolerant global database. The database should be coordinated and manipulated by advanced database management.

The database management should provide the following capabilities:

- Flexibility provided by database interface routines;
- Prevention of data loss due to power failures;
- Simplified method of creating, adding, deleting, modifying, and retrieving of files and documents;
- Easy retrieval of data for reporting, printing, displaying, and returning data to the database;
- On-line modification of database as the process is continuously monitored and controlled;
- Advanced data retrieval methods, retrieval via a range of criteria, based on associative retrieval and English written instructions:
- Automatically generated reports for plant management;
- Automatically removing obsolete data;
- Fault tolerant qualification for global memory resources;
- No major limitation to memory usage, especially concerning what is displayed or reported to the operator;
- Size adequate for future applications;
- Utilization of “packed digitals” to streamline and reduce overloading the system without sacrificing major features of the system.

7.9.2 Database Availability

To ensure high availability, the database of the distributed control system should be so organized that signals from redundant and independent communication networks are stored in independent memories. Such redundant signals should also be treated by at least two independent processors for the monitoring, quality checking, alarming, reporting, and MMI functions. Such a distribution can result in an excellent availability without increasing the cost for redundancy. Other distributions include utilizing redundant communication networks and processors that are reconfigurable, ring-bussed, fault tolerant, or two out of three voting schemes. Refer to Section 8 for details on availability calculations.

The network is the most frequently updated and universal source of data for all momentary values of process variables, when the system uses periodical reporting with routine broadcast. All data stations have simultaneous access to the updated values every few milliseconds or less.

7.9.3 Data Initiation and System Tagging

The plant-wide database should consist of all data input to the system from process sensors, calculated or transformed variables, internal distributed control system status and control signals, operator input constants, all output signals, and data resident in the system’s memories. It is suggested to the distributed control system manufacturer that, for consistency and proper interface, the user obtain a complete understanding of the manufacturer’s plant-wide database requirements. The importance of the work required to initiate, review, and interface this database cannot be stressed enough.

Copyright © 1991 IEEE All Rights Reserved

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS Not for Resale

When specifying the system, tagging the requirements and facilities of the specific distributed control system being used must be completely understood. The designers must consider tagging of the inputs, outputs, algorithms, ladder rungs, and control stations, etc. It is suggested that both ISA S5.3 [B2] and IEEE 806-1986 [B85] be utilized to the greatest practical extent. Cross referencing and interfacing throughout the documentation of the system should be understood and utilized. Manufacturers are strongly encouraged to design their system tagging to be compatible to the single plant-wide tagging system now being used throughout the power industry.

7.9.4 Engineering Units

A consistent and comprehensive set of engineering units, terms, and abbreviations should be set up early on any project. The engineering units decided upon will depend on the requirements of the designers, manufacturers, and end users. The important point is to be organized and consistent from the initial part of the project to avoid errors in the database later on. These units, terms, and abbreviations, once established, should be used consistently throughout the project documentation, on annunciator window engraving, nameplates, etc.

7.10 Data Acquisition and Preprocessing Functions

In the integrated system, there is a common but distributed database that services all data recipients. The data acquisition function also treated in Section 4 is the source of the database. Using the same data source for all functions ensures that these different functions are executed in congruency. Different data sources for the same process information should only be used if safety requirements strictly demand redundancy. An advantage of a functionally and/or geographically distributed control system is that it allows the database to be processed and stored throughout the system without need of a large mainframe computer. Preprocessing, also treated in Section 4, will occur at or near the I/O electronics of the system. Such operations as signal conditioning, conversion, compensation, scaling, limit checking, time tagging, open thermocouple detection, supervision, and alarming will occur here for both the control system and data acquisition system. Data can be collected from system I/O equipment, processors, and/or algorithm modules for display to the operators and for control of the processes. The distributed control system is essentially a distributed computer system.

A partitioned database in which declarative or nonvarying attributes such as service description, engineering units, etc., are stored in a library and only accessed when required for presentation to the operator is preferred. An active database consisting only of point name or address and time-dependent attributes such as current value and status will ease the communication task.

8. Reliability, Availability, and Fault Tolerance of Distributed Control and Monitoring Systems

8.1 Introduction

A basic understanding of reliability and availability of distributed control and monitoring systems is extremely important. The purpose of this section is to familiarize application engineers with utilizing the basic principles of reliability engineering and some of the fault tolerant approaches available. The engineer will be introduced to qualitative as well as quantitative techniques with application examples see [B60] , [B62] .

8.2 Overall View

Section 8 has its impact on Sections 4, 5, 6, and 7 and also extends into the field instrumentation and the mechanical equipment of the power plant. It is the intention of Section 8 to show that excellent reliability and availability of a

Copyright © 1991 IEEE All Rights Reserved

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS Not for Resale

power plant is the result of thorough understanding of the process, properly matched mechanical equipment, field instrumentation, and all aspects of the control and monitoring system as an integrated whole.

8.2.1 Semantic Synopsis

The structure of Section 8 is shown in Fig 16.

8.3 Reliability

The old saying the chain is as strong as the weakest link is directly applicable to the reliability of a control and monitoring system. The link consists of a microelectronic element (hardware), software element, and the human element. All three elements of concern must be considered as an integrated system design.

The engineer must strive for a dependable system design. That is, a system has “dependability” when reliability, availability, and quality are integrated into the system design. These three items are closely coupled together. Reliability is a probability of success. It is the probability that the particular piece of equipment or element will perform its purpose adequately for the designed time period, and under the various operating conditions the equipment or element encounters. Availability is the characteristic of a piece of equipment or element expressed by the probability that it will be operational at a randomly selected future instant in time see [B60] . Quality is much more difficult to define. It has a peculiar and essential character with a high degree of excellence to assure that weak areas of design are eliminated and defective components are not utilized in the system.

Finding weak areas in a distributed control system design is not an easy task. A state-of-the-art approach for the utility industry for finding weak areas of system design is failure mode effect analysis (FMEA) and fault tree analysis (FTA).

8.3.1 Purpose and Scope of Failure Mode Effect Analysis (FMEA) and Fault Tree Analysis (FTA)

The main purpose of the FMEA and FTA is to isolate and identify weaknesses in the control system design, and to provide appropriate preventive measures such as hot repair, redundancy, partitioning, fault tolerance with self diagnostics, and available spare parts so that the problem area can be repaired quickly. An adequately implemented FMEA and FTA analysis enhances the dependability of a distributed control system. For examples of FMEA and FTA, refer to Appendix B.

8.3.2 Questions Answered by FMEA

The following questions will be answered by FMEA.

A) How can each part or card module conceivably fail?
B) What mechanism might produce these modes of failure?
C) What could the effect be if the failure did occur?
D) Is the failure in the safe or unsafe direction?
E) Does the failure contribute to loss of total or partial unit availability?
F) How does the failure decrease unit operability?
G) How is the failure detected?
H) What preventative measures are taken to compensate for the failure?
I) What will it cost to implement the preventive measures?

8.3.2.1 Advantages and Disadvantages of a FMEA

The following are a few of the major items connected with FMEAs.

1) Advantages of an FMEA
   a) It identifies critical components easily.

Copyright © 1991 IEEE All Rights Reserved

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS Not for Resale

b) It provides some guidance as to the order in which preventative measures should be implemented.
c) It may help find a hazardous occurrence that is not obvious to the analyst or control system designer.
d) It familiarizes the analyst with details of the instrumentation and control system.
e) It provides historical documentation for future reference to aid in analysis of field failures and consideration of design changes.
f) It assists in the objective evaluation of design requirements related to hot repair, redundancy, failure detection system, fail safe characteristics and automatic and manual override.
g) It can be utilized during factory check-out of the control system.

2) Disadvantages of a FMEA
a) Multiple failures are not considered.
b) It is not readily apparent how subsystems and systems interact with each other.
These weaknesses are eliminated by utilizing a fault tree analysis (FTA).

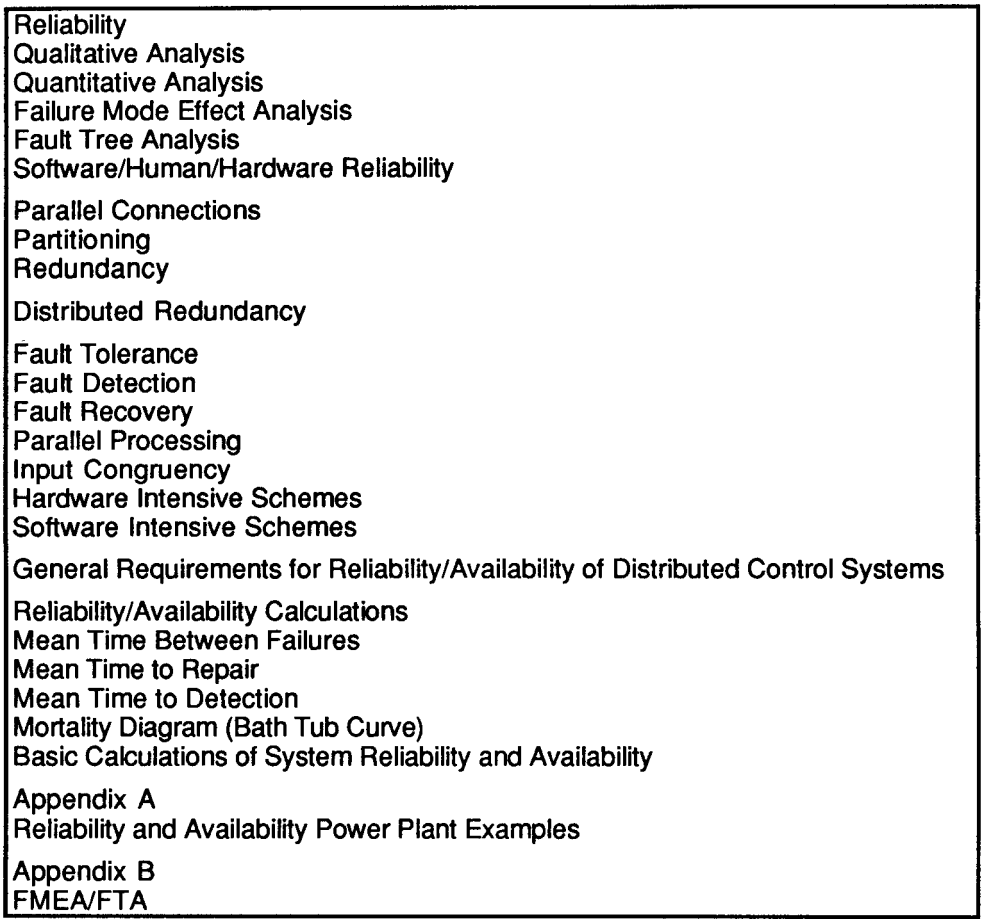


Figure 16—Semantic Synopsis

8.3.3 Fault Tree Analysis (FTA)

One way to diagram and relate the information developed in a failure mode effect analysis is to utilize a fault tree.

A fault tree is a logic diagram that describes what combination of component (module) failures will cause a top event to occur. This is different from the FMEA that starts at the component (module) level and attempts to determine what top event will result from a specific component (module) failure.

Copyright © 1991 IEEE All Rights Reserved

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS Not for Resale

For each top event chosen, a fault tree can be constructed. Not only does this tree provide a logic aid that illustrates component (modules) interaction and other system interactions, it can also be used with Boolean Algebra and failure rate data for each component (module) to determine the probability of occurrence of the top event see [B63] . A qualitative approach is also desirable and very beneficial and would yield:

1) True redundancy available in the control system and interlock logic
2) Where redundancy is needed
3) What single component failures are present
4) What are the common cause failures
5) System trouble-shooting aid for instrument repair and operating personnel
6) Assist operators and maintenance personnel in understanding over-all system interactions.

The main disadvantage of fault tree analysis is that it may not be easy to determine the top event. That is why the FMEA is utilized.

Some examples of top events on the fault tree are:

1) Explosion
2) Implosion
3) Water induction to the turbine
4) Loss of all CRT information to the operator.

Figure B2 in Appendix B illustrates a general fault tree for a system failure. This figure emphasizes looking at software failures, mechanical failures, human error, electrical failures and environmental stress.

8.4 Software/Human/Hardware Reliability

In general a distributed control system can fail in several ways:

1) Hardware electronics card and/or plugin connector failure.
2) Interfacing problems between systems and components (for example, timing and general communication)
3) Environmental stress (temperature, humidity, wet faults, etc.)
4) Human error in operation, maintenance and design.
5) Software failures

8.4.1 Software Control Failures

These failures include:

1) Failure to perform a required function; that is, the control function is never executed or no answer is produced.
2) Performing a function not required; that is, producing a wrong answer or producing a right answer but under inappropriate conditions. For example, activating a motor-operated valve inadvertently too late, too early, or failing to cease a process operation at a prescribed time.
3) Timing or sequencing problem. For example, it may be necessary to ensure that two things happen at the same time, at different times, or in a particular order.
4) Failure to recognize a hazardous or failing condition requiring corrective action.
5) Producing the wrong response to a hazardous condition.

Copyright © 1991 IEEE All Rights Reserved

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS Not for Resale

8.4.1.1 Quality Assurance of Software

The hardware reliability is justification for thinking that certain complex devices might follow an exponential law. In such a case, the mean time to failure (or failure rate) totally describes the failure behavior. Unfortunately, such justification does not apply to software.

The goal should be to reduce the failure probability of the computer software. A failure is defined as the inability of the software (code) to provide the correct solution (action) or inability of the user to apply software correctly. In order to better assure ourselves of a highly reliable code, utilities should have the vendor explain in detail how they provide quality assurance of their software [B65] , [B66] .

8.4.2 Human Reliability

One definition of human reliability is the probability of successful performance of the human activities necessary either for a reliable or an available system see [B68] . Human error may take place during the design, operation or maintenance phase of the over-all system activities as illustrated in Fig B2 in Appendix B. To enhance the human reliability of the system, one must design the distributed control system to match the capabilities and the limitations of the human operator. In other words, human factors engineering principles must be applied in the following areas of concern: (1) man/machine interface, (2) workstation design, and (3) overall environmental considerations. For more details concerning the man/machine interface, see Section 7, Data Acquisition and Monitoring see [B69] through [B71] , [B79] , [B82] .

8.5 Partitioning, Redundancy, and Fault Tolerance

8.5.1 Introduction

The ability of a system to maintain its design functionality in the event of an internal fault of one or more of its individual elements is a long sought-after goal of system designers. The use of computer technology in the area of process control and information management has given rise to a number of architectural, hardware, and software techniques that greatly enhance a system’s tolerance to single, and in some cases, multiple element faults. Collectively, these schemes and techniques are known as fault tolerant technology.

The distributed control and monitoring systems avail various means to meet the specified reliability and availability. With the currently available technology, the most important means is to ensure a very high quality of components used for building the system. In some critical cases, Mil-Spec components should be utilized. Other collateral means consist of partitioning and distributed redundancy (see 8.5.2 and 8.5.3). In most cases, such techniques will satisfy the reliability criteria. Also, computer technology has evolved to a point where fault tolerant techniques are becoming increasingly affordable, offering an additional degree of reliability (see 8.6.1).

No matter how sophisticated a fault tolerant technique used, any system cannot reach 100% availability, but can push the availability nearer to that end at the expense of capital investment. A higher availability may pay back, in time, the investment cost by possibly avoiding forced outages, nuisance trips, and reducing maintenance and operational costs. A detailed evaluation of the availability and cost will eventually set the availability specification for a specific application.

8.5.2 Partitioning

The first mechanism required for any fault tolerant system is the element of system partitioning. The partitioning must provide isolation of these subsystems such that a fault of any single subsystem will not propagate into its functional or physical neighbors.

Generally, partitioning in combination with redundancy will fulfill the definition of fault tolerance as the ability of a system to maintain its designed functionality on the occurrence of failure. In some cases, partitioning alone may

Copyright © 1991 IEEE All Rights Reserved

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS Not for Resale

provide the required degree of fault tolerance by restricting a fault to an acceptable portion of the total system, wherein the designed functionality of the process can be maintained, though possibly at a reduced operative level.

An example of when partitioning may provide adequate fault tolerance is the case of pulverized coal mill control. The loss of one mill in a plant may limit the plant, but it generally will not result in the plant coming off line. For mill protection and safety, however, partitioning alone is not adequate (see discussion on processor and I/O redundancy).

A loosely coupled system provides better fault isolation than a tightly coupled system. With reduced interaction, the probability of one processor failure affecting multi-processor functionality is reduced.

Early direct digital control (DDC) systems were implemented using mainframe computers. In such systems, the hardware partitioning was contained in the entire mainframe. In order to provide even the minimal single element failure safeguard, these systems required another mainframe for redundancy. As the number of components with one system was very large, the MTBF was adversely affected. Each failure meant the disruption of all control functions at a time. Modern distributed systems may have an even larger number of total components, but because of partitioning, only a smaller number of functions will be disrupted by a single fault. Partitioning is a mechanism used also by fault tolerant systems, to which other methods are added. A common mechanism for both distributed and fault tolerant systems is redundancy.

8.5.3 Redundancy

Redundancy is the duplication of resources required to provide a given function. This redundancy may be provided by duplication of hardware or software or by the reassignment of the existing resource within the system. In the mainframe systems of earlier technology, redundancy could only be achieved by the use of duplicate hardware (another mainframe); this was due to the partitioning boundaries established. While a number of systems were successfully implemented, and are currently operational using this approach, there is ongoing concern over the fact that in the implementation of this redundant control scheme, there exists the need for a switching mechanism. Therefore, a single failure can bring down the entire system (see also the common mode failure example in Appendix A).

The mainframe example has been presented in order to typify some major mechanisms and potential liabilities that fault tolerant technology must transcend. Current approaches to fault tolerant systems make use of hybrid mixture of these basic elements to achieve their desired system availability goal. Advances in micro-processor capabilities and reductions in the cost of computational resources now allow system functionality to be achieved through the use of many smaller computational elements, as opposed to one or several large elements. Partitioning and distributed redundancy is a means whereby the physical and functional grouping is reduced to much smaller size. The fault tolerant engineering goal is to reduce the scope of any single element function to a point where the loss of that resource will not catastrophically effect total system functionality.

Once partitioning boundaries have been established, the resultant elements can be reviewed with respect to identifying those elements whose individual failure mode would have an unacceptable effect on the total system. Any element that is determined to be either of critical importance or that possesses unacceptable mean-time-between-failures (MTBF) can be marked for application of redundant techniques. It should be remembered that almost any method of implementing redundancy will adversely affect the cost-effectiveness of the system. Therefore, it is important to properly identify those areas of any system in which redundancy is to be implemented. Failure mode effect analysis and fault tree analysis are excellent tools to be utilized in determining partitioning and redundancy requirements. Distributed systems lend themselves to flexible implementation of redundancy on a need basis throughout the plant, therefore, redundancy is also distributed on a modular selective basis. The hardware is partitioned following the functional, geographical, and fault isolation criteria. In the evaluation of redundancy needs, increased capital equipment costs of the system should be weighed against increased availability, safety, and cost of a forced outage. Distributed systems offer the possibility to add redundancy only to the essential parts of the plant harmoniously matched with the mechanical equipment functionality so the redundancy follows the functional distribution criteria.

Many plant subsystems are redundant. Distributed redundancy, along with partitioning, could be used by the allotment of individual controllers to each segment of equipment of the redundant subsystem.

Copyright © 1991 IEEE All Rights Reserved

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS Not for Resale

A standby configuration will include both the mechanical equipment and the controller. Such a configuration has the advantage that any fault of either equipment or controller will have the backup of the standby subsystem. Another advantage of such a configuration consists of the fact that a segment of the subsystem is always available for repairs or maintenance. Backup activation shall be initiated and supervised automatically with an option to do manually.

Some of the essential plant equipment does not have redundancy. For such equipment, a modular control redundancy that works under the fault tolerant principles, as treated in 8.6, is suggested.

Irrespective of the fact that a processor is redundant or not, the processor shall have self-testing and diagnostic facility with an appropriate means of annunciating its availability state as well as its capability to communicate effectively with its I/O. For dual redundant systems, in addition to self-testing, a degree of cross-checking may be advantageous, but care in evaluating single failures should be considered either in the checker or system. The same should apply in the case of triple redundant controllers with 2 out of 3 voting logic, where the voting circuitry and other hardware should be evaluated for possible common mode failure elements.

8.6 Fault Tolerance

To define “fault tolerance” one must first explain “fault.” A fault is a cause that produces an error within the system. Thus, a fault brings a system into an erroneous state that can lead to a failure. A failure is a situation where the system can no longer safely perform all its functions. The quality of a system to cope with faults occurring within the system, so that specified services are maintained, is considered fault tolerance. From this perspective, there can be many degrees and types of fault tolerance systems. This Guide is addressing itself to distributed control and monitoring systems. From this perspective, fault tolerance is considered the ability of the system (control and monitoring) to act, such that a fault event is transparent to the controlled process and the human operators, and the controlled plant remains safely in service.

Whenever designing a fault tolerant system one should review the entire scope of the system. This includes sensors, the control system, and final devices. The content of this subsection is to review fault tolerance with respect to the control and monitoring systems. The key word here is systems. Thus, we are directing ourselves toward what happens when faults occur within the control or monitoring systems or both as shown in Fig 17. There are fault tolerant schemes that are process specific. An example would be detection of a failed transmitter and changing the control strategy so the system can continue to operate. An example of this would be the replacement of a failed measured variable with that of a calculated value.

Since, by definition, a fault tolerant system is one in which a fault-event is transparent to the controlled process and human operators, it is apparent that, first, we are addressing our-selves to modern digital systems. Second, we are addressing ourselves to faults that occur within the control and monitoring system and not the field devices such as transmitters or final actuators. If a fault manifests itself by providing the wrong output, or the right output at the wrong time, it is called noninteger. If the system stops providing any output, it is called non-steady.

For a system to be fault tolerant, it must be able to detect the fault. There are basically three approaches to fault detection. The first is independent self-testing and self-diagnostics by all processors. The second is the use of a checker that makes use of a separate processor to verify operation of another or several processors. The third technique is called replicated processing, which is the simultaneous processing of the same program with identical data by more than one processor with a comparison of the results. Both the checker and the replicated processing techniques also typically incorporate self-diagnostics.

Once a fault has been detected, it should be annunciated so that a repair can be quickly initiated. As long as a fault exists, the system works with an increased risk of forced outage until the system is totally restored, meaning that it works with all design resources.

Copyright © 1991 IEEE All Rights Reserved

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS Not for Resale

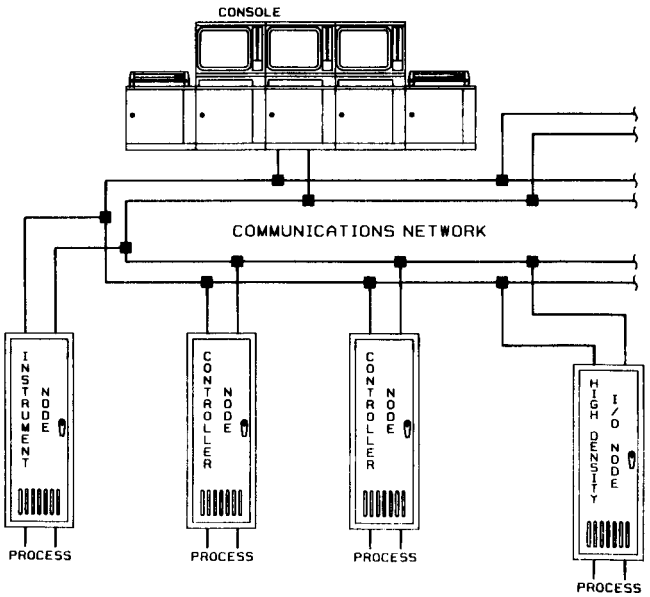


Figure 17—Control and Monitoring System Overview

When a fault occurs, three transients are introduced into the system. First, of course, is the occurrence of the fault. The second transient occurs when the source of the fault is removed from the system. The final transient occurs when the faulty element is replaced with a new or repaired element. All three of these transients must be transparent to the process, by definition, for the system to be considered fault tolerant.

In the future, we can expect fault-tolerant techniques to be increasingly adopted by distributed control and monitoring systems. The prime initiate in an increasing use of fault-tolerant techniques is their decreasing cost. Hardware cost is continuously decreasing, promoted by advances in technology. Also, the software needed for fault tolerance is becoming more established. This results in an increase in sophistication and commercial availability, with the end result being that the software is also becoming more affordable.

8.6.1 Fault-Tolerant Techniques

In essence there are two fault-tolerant techniques: one is hardware-intensive, while the other is software-intensive, as shown in Fig 18. The use of redundant processors, where upon fault detection a backup processor takes over, is an example of a hardware intensive approach. Figure 18a shows a scheme utilizing a dedicated backup processor. The scheme in Fig 18b shows a shared backup processor within a controller subsystem employing a number of control modules communicating on a local redundant serial bus. Another approach is replicated processing. This is a technique where two or more processors perform the same program with identical inputs. Tightly coupled parallel processors require that the program execution be synchronized such that each group of instructions is completed by each processor, with cross-checking occurring before proceeding to the next group of instructions.

Loosely coupled parallel processor configurations only compare final results; synchronization, obviously, is no longer possible. Any kind of switch is avoided.

An extension and modification of this technique covers selective I/O redundancy, particularly in association with discrete logic on safety applications.

Software intensive schemes for fault tolerance (Fig 18c) use the approach that any program segment can be loaded and run on any available processor. Upon fault detection, the faulty processor is removed from service. The system program is then run in the remaining processors. Even though this approach is called software intensive, it can require

Copyright © 1991 IEEE All Rights Reserved

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS Not for Resale

additional hardware, since for this approach to work, the processors cannot be fully loaded or else they would not be able to pick-up and run the program from a faulty processor.

Another example of a fault-tolerant technique consists of strictly separating the controls of redundant plant equipment, physically and functionally, and separating manual and automatic control in the same way; thus, a single fault never inhibits manual and automatic control at the same time and never inhibits control of both redundancies in the plant at the same time see [B80] , [B81] .

8.7 General Requirement for Reliability/ Availability of Distributed Control System

8.7.1 Over-All Plant Availability

Establish an over-all plant availability and reliability number in the power plant charter or specification. This will be the “target” or goal to be satisfied by the chemical, control, electrical, and mechanical systems, etc. In order to meet this target goal, the distributed control system will have to be higher in reliability and availability, since it is only one major component of the total system.

8.7.2 Dynamic Maintenance (Hot Repair)

Hot repair or dynamic maintenance is essential for highly available systems. The replacement of a piece of equipment, printed circuit card, or data station while the system remains operational is desired.

8.7.3 Reliability of Basic Network Topology—Star, Ring, Bus, and Tree Topologies—Gateways

8.7.3.1 Star Topology

In star topology, each data station is connected by a point-to-point link to a common active central switch. This topology exhibits a centralized communications control strategy. A “star hub” can link buses or links. In general, the central switch mode is rather complex. A single failure of the central switch may bring down the entire system. This topology should be utilized judiciously. “Star hubs” for bus extensions or rings with centralized switching devices are not used for power plant control as of this printing. Instead, redundant computers that link bus or ring segments are frequently used for power plant control.

8.7.3.2 Ring Topology

In the ring topology, the communication network is connected in point-to-point manner to each node, with each node acting as a repeater. A failure of a repeater may disable the system. Node bypass into redundant media with associated interfaces are, therefore, effectively employed and suggested.

Ring topology is favorably suited for fiber optical transmission. This approach may be helpful for an application that has an extremely high electrical noise environment.

8.7.3.3 Bus Topology

The bus topology is a very different approach as compared to the star and ring topology. In this approach, the communications network is simply the transmission medium—no switches and no repeaters. All data stations attach, through appropriate hardware interfacing, directly to a linear transmission medium or bus. The tree topology is a generalization of the bus topology. Even though the bus/tree topology appears to be more flexible, a single failure, such as a break in the cable, can disable a large part or all of the system. Redundant cable is recommended.

Copyright © 1991 IEEE All Rights Reserved

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS Not for Resale

8.7.3.4 Gateways

The application of a gateway within a control system may reduce the hardware, software, and human reliability of the system. At times, however, the utilization of a gateway is necessary and justified. A gateway is a device connecting two computer systems that usually use different protocols, or connect two independent networks. A gateway may slow down the response time of data flow, which may have a negative effect on the operator making a timely decision. However, in a continuous development effort, faster gateway response time implementation is anticipated. It is suggested that when gateway utilization is considered, a response time analysis is conducted to see whether overall application requirements are met. A gateway constitutes an extra component that could fail, and if the two interconnected systems are interdependent serially, then reduced reliability could result. If the two systems are autonomous in their control execution and the connection serves a data acquisition function, then the impact on reliability is lessened. Like any other element in the system, the gateway is subject to FMEA and FTA analysis to identify the impact of failure on total system performance. The analysis should help determine whether the gateway functionality is adequate, whether redundancy should be employed, or use of gateway be avoided.

8.7.4 Reliability of Broadband vs. Baseband

For power plant application, it is preferred that the baseband transmission method be utilized. It is basically more reliable than a broadband topology. Refer to Figs 19 and 20. The broadband cable network is less reliable because of the double length and the vulnerability of the head-end. A head-end failure may bring down the entire network. Again, it depends on the application and the particular broadband approach. Broadband may adequately satisfy the design criteria.

8.8 Introduction to Reliability/Availability Calculations

Reliability is a probability of success. It is the probability that the particular piece of equipment or item will perform its purpose adequately for the designed time period and under the various operating conditions the equipment encounters.

The frequency at which failures or malfunctions occurs in the equipment is used as a parameter for the mathematical formulation of reliability. This parameter is called failure rate. It is usually measured in number of failures per unit operating hour. Its reciprocal is called the mean time between failure (MTBF) and is measured in hours.

Reliability can also be expressed mathematically as:

$R(t) = e^{-\int_0^t \lambda dt}$

R = Reliability

λ = Failure Rate

8.8.1 Mortality Diagram (Bath Tub Curve)

Reliability distinguishes three characteristic types of failure. They are early failures, random failures and wearout failures. Figure 21, which illustrates the failure pattern that occurs during equipment operating life, is typically called the “bath tub” curve or mortality diagram.

Typically, “early failures” result from poor manufacturing and quality control techniques during the production process. Early failures also occur because of poor assembly of equipment. This part of the mortality diagram can be greatly reduced by applying a burn-in procedure to the components and equipment.

The burn-in process consists of operating the equipment for a number of hours under conditions simulating actual use. The early failures are replaced by good components and assembly errors are found during the burn-in process. The vendors are to explain in detail how they burn-in their systems and components. It is suggested that thermal cycling of

Copyright © 1991 IEEE All Rights Reserved

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS Not for Resale

each production unit and random vibration qualification testing for at least the prototypes be utilized by the vendors or their subcontractors to eliminate early failure rates see [B72] .

Moving across the mortality diagram, it becomes noticeable that random failures or chance failures are at a constant failure rate. These failures have occurred because sudden stresses have been applied to the component(s) that were beyond the design strength of the component(s). Good burn-in techniques and maintenance procedures will not eliminate chance failures of the component(s) in major equipment. *Note*: This part of diagram represents constant failure rates and reliability is mathematically represented by:

$$R(t) = e^{-\lambda t}$$

The last part of the “bath tub” curve is the wear-out failure. These failures are caused by the wear-out of the component(s). These occur when the equipment is not properly maintained or not maintained at all.

It is essential that high reliability is designed within the distributed control system. mean time between failure data by itself does not insure high reliability. High mean time between failure data must be provided with how the vendor derates the critical components of their system see [B75] . Derating for electrical, mechanical or electromechanical parts is defined as the practice of reducing the electrical, mechanical or environmental operating stress below the maximum levels that the part is capable of sustaining in order to increase application reliability.

It is important that both the reliability and availability elements be examined. Availability or reliability calculations by themselves are very misleading. For example, mean time to repair can be very low; combined with poor reliability, it can give the impression of a highly available system, but in actuality, the system is unreliable. Likewise, the system can be extremely reliable, a high mean time between failures, combined with a long mean time to repair, to give the impression of a highly available system, but in actuality, the system is so complex to repair that the availability is extremely low.

Copyright © 1991 IEEE All Rights Reserved

--`,,`-`-`,,`,,`,`,,`---

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS Not for Resale

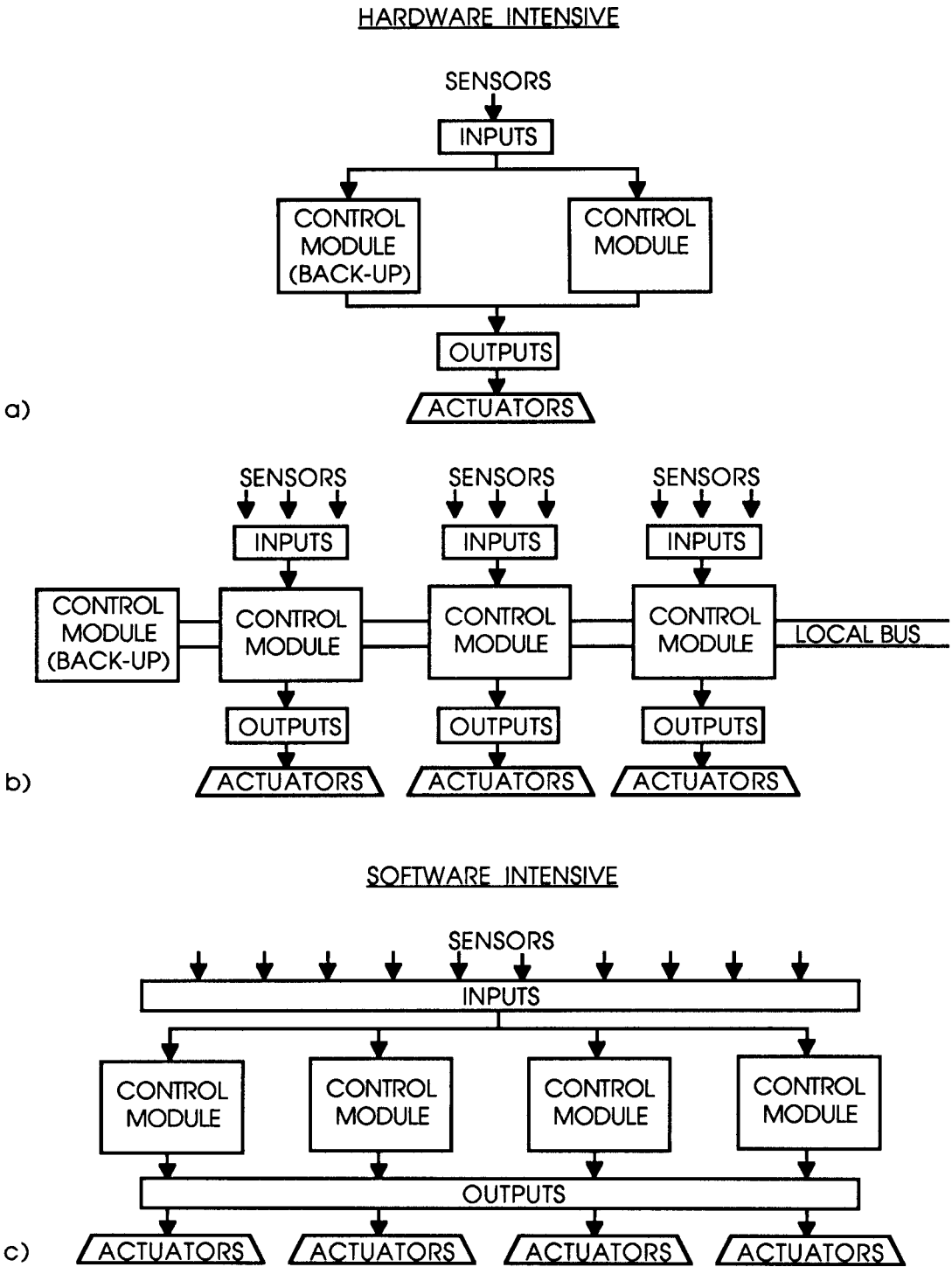


Figure 18—Redundancy Schemes

Copyright © 1991 IEEE All Rights Reserved

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS
Not for Resale

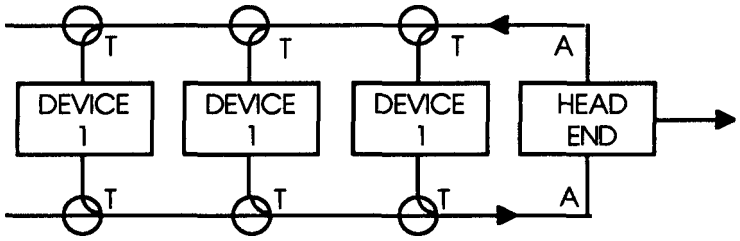
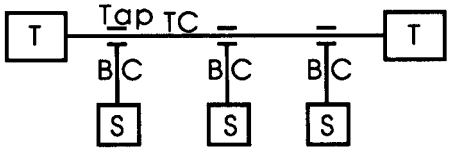


Figure 19—Broadband Configuration



T = TERMINATER BC = BRANCH (DROP) CABLE
TC = TRUNK CABLE S = STATION

Figure 20—Baseband Configuration

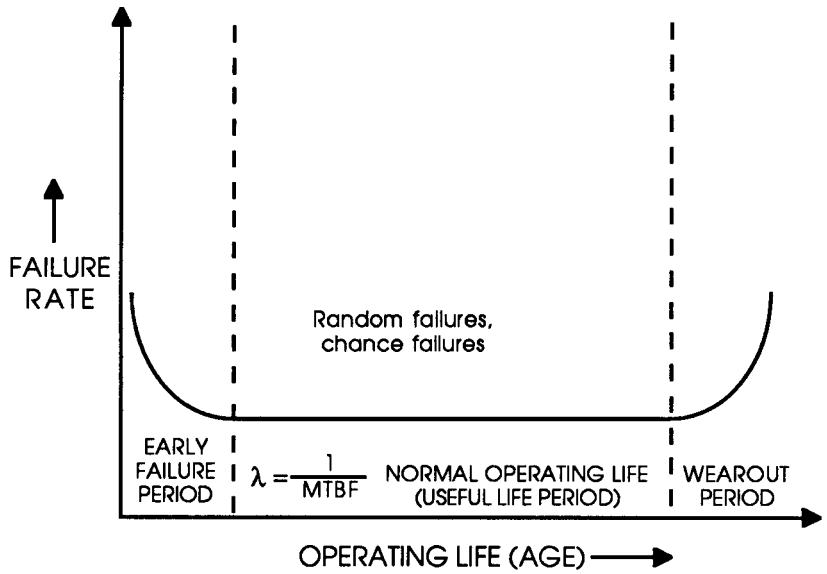


Figure 21—Mortality Diagram

Copyright © 1991 IEEE All Rights Reserved

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS
Not for Resale

9. Bibliography

[B1] Gerry, John P. A Comparison of PID Control Algorithms. *Control Engineering*, March, 1987, pp 102–105.

[B2] ISA S5.3, Flow Diagram Graphic Symbols for Distributed Control/Shared Display Instrumentation Logic and Computer Systems.

[B3] IEEE Std 1046-1991, IEEE Application Guide Tutorial, Distributed Control and Monitoring for Power Generating Stations. The Institute of Electrical and Electronics Engineers, Inc., New York, 1985.

[B4] Damsker, D. J. Reliability and Speed: Major Performance Criteria of Distributed Control. *IEEE Transactions on Power Apparatus and Systems*, vol. PAS-104, No. 3, March 1985.

[B5] Damsker, D. "Integrated as opposed to segregated power plant distributed control." Paper presented at ISA POWID Symposium, Cleveland, Ohio, May, 1986.

[B6] EPRI NP-254, *Study of Remote Multiplexing for Power Plant Applications, Volume II, Final Report.* Prepared by United Engineers and Constructors, Inc., July, 1976.

[B7] ISO/JT-1 7498, OSI Reference Model, Parts 1–4.

[B8] ISA-S72.01-1985, PROWAY-LAN Industrial Data Highway.

[B9] Damsker, D. J. Distributed Control Messages, Their Security and Efficiency. *IEEE Transactions*, PAS-103, No. 8, August 1984, pp. 2058–2065.

[B10] EPRI NP-254, *Study of Remote Multiplexing for Power Plant Applications, Volume I, Final Report*. Prepared by TRW Systems and Energy Group, July, 1976.

[B11] IEEE Std 518-1982, IEEE Guide for the Installation of Electrical Equipment to Minimize Noise Inputs to Controllers from External Sources. (ANSI)

[B12] IEC Publication 79-10 (1972) Part 10: Classification of Hazardous Areas.

[B13] IEC Publication 79-1 (1971) Part 1: Construction and Test of Flameproof Enclosures of Electrical Apparatus.

[B14] IEC Publication 79-3 (1972) Part 3: Spark Test Apparatus for Intrinsically Safe Circuits.

[B15] IEC Publication 79-11 (1984) Part 11: Construction and Test of Intrinsically Safe and Associated Apparatus.

[B16] IEEE Std 383-1974 (R1980), IEEE Standard for Type Test of Class 1E Electric Cable, Field Splices, and Connections for Nuclear Power Generating Systems. (See Section 2.5, "Flame Tests.") (ANSI)

[B17] Jones, Clarence T. Programmable Controllers; Concepts and Applications, International Procontrols, 1983.

[B18] Hammond, Joseph L. and O'Reilly, Peter J. P. *Performance Analysis of Local Computer Networks.* Addison-Wesley Publishing Company, 1986.

[B19] Whitman, S. and Webster, E. "Transmitters: Key to Instrument Accuracy," *Power*, April 1987, pp. 63–66.

[B20] Armstrong, C. "Smart Actuators," ISA, Houston, Oct 1987, Session 17.

[B21] Laduzinsky, A. J. Modular Signal Conditioning. *Control Engineering*, Sept 1986, pp. 154–155.

Copyright © 1991 IEEE All Rights Reserved

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS Not for Resale

[B22] Bailey, S. J. Process-Embedded Decision Booms. *Control Engineering*, Nov 1986, pp. 80–85.

[B23] Babb, M. New Graphics Software for Process Control. *Control Engineering*, Jan. 1987, pp. 92–94.

[B24] d'Epinay, Th. Lalive, et. al. "Architecture for Process Control," from *Computer Systems for Process Control*," Plenum Press, 1986, pp. 109–140.

[B25] Winard, H. Microcontrollers. *Electronic Design*, Nov, pp. 167–169.

[B26] Hornstein, J. V. Parallel Processing Attacks Real Time World. *MiniMicro Systems*, Dec 1986, pp. 65–77.

[B27] Cleveland, P. What's Happening With A/D and D/A Converters?, *I & CS*, Dec 1986, pp. 21–24.

[B28] IEEE Std 802-1990, *IEEE Standards for Local and Metropolitan Area Networks: Overview and Architecture.* IEEE Std 802.1D-1990, *IEEE Standards for Local and Metropolitan Area Networks: Media Access Control (MAC) Bridges.* IEEE Std 802.1E-1990, *IEEE Standards for Local and Metropolitan Area Networks: System Load Protocol.* ISO 8802-2 : 1989, *Information Processing Systems —Local Area Networks—Part 2: Logical Link Control.* ISO 8802-3 : 1990-2, *Information Processing Systems —Local Area Networks—Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications.* IEEE Std 802.3b,c,d,e-1989, *IEEE Supplements to Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications.* IEEE Std 802.3h-1990, *IEEE Supplement to Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications: Layer Management.* IEEE Std 802.3i-1990, *IEEE Supplement to Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications: System Considerations for Multisegment 10 Mb/s Baseband Networks (Section 13) and Twisted-Pair Medium Attachment Unit (Mau) and Baseband Medium, Type 10BASE-T (Section 14).* ISO 8802-4 : 1990, *Information Processing Systems —Local Area Networks—Part 4: Token-Passing Bus Access Method and Physical Layer Specifications.* IEEE Std 802.5-1989, *IEEE Standards for Local Area Networks: Token Ring Access Method and Physical Layer Specifications.* IEEE Std 802.7-1989, *IEEE Recommended Practices for Broadband Local Area Networks.*

[B29] Damsker, D. J., coordinator. "Control Data Networks." IEEE Tutorial Course, 86 EH0240-2-PWR, 1986.

[B30] Damsker, D. J. "Assessment of Industrial Data Network Standards." IEEE 87SM410-4, San Francisco, July 87.

[B31] Damsker, D. J. "Information Consistency and OSI-Based Control Networks." ISA, POWID Symposium, Rochester, NY, May 1987.

[B32] Damsker, D. J. Fiber Optic Links for Power Plant Control. *Power Engineering*, Feb 1982, pp. 53—57.

[B33] IEEE Document 83TH0104-0PWR, *Fiber Optic Applications in Electrical Substations.*

[B34] Berry, D. Distributed Intelligence in Process Control. *Control Engineering*, May 1987, pp. 62—64.

[B35] Damsker, D. J. Reliability and Speed, Major Performance Criteria of Distributed Control. *IEEE Transactions* PAS-104, no 3, March 1985, pp. 538—542.

[B36] Damsker, D. J. "Critique to MAP and PROWAY." IFAC Workshop on "Distributed Computer Control Systems," Mayschoss, W. Germany, Oct 1—3,1986.

[B37] Damsker, D. J. Integrated as Opposed to Segregated Distributed Controls. ISA, Instrumentation in the Power Industry, vol 29, 1986, pp. 65—73.

[B38] Whitaker, E. J. and Schutz, H. A. Data Sharing on EPA or MiniMAP Subnetworks. *Control Engineering*, June 1987, pp. 156—160.

Copyright © 1991 IEEE All Rights Reserved

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS Not for Resale

[B39] Miller, N. et. al., “MAP User/Vendor Panel. *InTech,* August 1987, pp. 9—13.

[B40] Kompass, E. J. Bailey’s INFI 90. *Control Engineering.* September 1988, vol 2, pp. 4—7.

[B41] Wood, G. G. International Standards. *Control Engineering*, Oct 1988, vol 2, pp. 22—25.

[B42] Babb, Michael. Alarms and Annunciators, Keeping the Lid On in Industrial Control. *Control Engineering*, Feb 1986.

[B43] Bayless, James W., Fishbein, Joseph, and Webre, John F. “Power Plant Automation via a Hierarchical, Distributed Microprocessor-Based Control System.” Paper presented at the 1983 ISA Power Industry Symposium, May 15–18, 1983.

[B44] Modern Control Room Concept for Power Plants. Brown Boveri Publication DKW 80985E.

[B45] Candel, J. “Control Room Design for Thermal Power Plants-Considerations for a Modern Concept,” Brown Boveri Publication No. CH-T020113E.

[B46] Damsker, Doral J. “Information Consistency and OSI-Based Control Data Networks,” paper presented at the 1987 ISA Power industry Symposium. May 21–23. 1987.

[B47] Hanbabe, P. and Motz, F. *Control of Power Plants with the Aid of Processed Information.* Brown Boveri Publication CHT100273E.

[B48] Kratochivil, J. *Control and Monitoring Equipment for the Power Plant Amer/O (Netherlands).* Brown Boveri Publication CHT100293E.

[B49] Krigman, Alan. Alarms; Operators; and Other Nuisances; Cope…or Court Catastrophe. *InTech*, December 1985.

[B50] Morris, Henry M. Alarming with Serial Signals. *Control Engineering*, May 1986.

[B51] Motz, F., Marzendorfer, M., and Menzel, H. Automation and Control Equipment for the Meirama Power Plant in Spain. Brown Boveri Review Publication 8/9, vol 68, Aug/Sept 1981.

[B52] Schellekens, Peter L. Alarm Management in Distributed Control Systems. *Control Engineering*, December 1984.

[B53] Shaw, John A. Smart Alarm Systems: Where Do We Go From Here? *InTech*, December 1985.

[B54] Shaw, John A. “Applications for Artificial Intelligence in Alarm Systems.” Combustion Engineering, Taylor Instrument, Rochester, New York.

[B55] Sierck, Henry A., Jr. “Methods for Comparison of Distributed Controls.” Paper presented at the 1987 ISA Power Industry Symposium, May 21–23, 1987.

[B56] Tylee, J. Louis. Model-Based Approaches to Instrument Failure Detection. *InTech,* Dec 1985.

[B57] Shirley, Richard S. *A Fog Index for CRT Displays (How Good Is Your CRT Display ?).* The Foxboro Company.

[B58] Eulinger, Ronald D. and King, James W. Performance Monitoring with Plant Instrumentation. Presented at POWID 32nd Annual Power Instrumentation Symposium, May 22–24, 1989.

Copyright © 1991 IEEE All Rights Reserved

--`,,`-`-`,,`,,`,`,`,,`---

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS Not for Resale

[B59] Beum, Holly, Brown, Gerald R., Federlein, James H., and Vierling, Jay. Control System Design, Part 4—The Man/Machine Interface. *InTech*, August 1989.

[B60] IEEE Std 352-1987, IEEE Guide for General Principles of Reliability Analysis of Nuclear Power Generating Station Safety Systems. (ANSI)

[B61] Schabowsky, Richard S. Jr. On the Evaluation and Validation of Fault-Tolerant Digital Control Systems. Presented at EPRI Seminar: Power Plant Digital Control and Fault-Tolerant Microcomputers, Scotsdale, Arizona, April 9, 1985.

[B62] Go Methodology. EPRI, Risk Assessment Program, vols 1 and 2, June 1983.

[B63] Fault Tree Handbook. NUREG-0492, Jan 1981.

[B64] Stallings, William. Local Networks. Macmillan Publishing Company, 1984, pp 326–336.

[B65] Reifer, Donald J. Software Failure Mode and Effects Analysis. *IEEE Transactions on Reliability*, Vol. R-28, No. 3, August 1979.

[B66] IEEE Software Standards: IEEE Std 610.12-1990, IEEE Standard Glossary of Software Engineering Terminology; IEEE Std 730-1989, IEEE Standard for Software Quality Assurance Plans (ANSI); IEEE Std 828-1983, IEEE Standard for Software Configuration Management Plans (ANSI); IEEE Std 829-1983, IEEE Standard for Software Test Documentation (ANSI); and IEEE Std 830-1984, IEEE Guide for Software Requirements Specifications (ANSI).

[B67] Swain, A. D., and Guttmann, H. E. Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications. NUREG/CR-1278, April 1980.

[B68] Guidelines for Control Room Design Reviews. NUREG-0700, Sept 1981.

[B69] Vancott, Harold P., and Kinkade, Robert G., Human Engineering Guide to Equipment Design, 1972. American Institutes for Research, Washington D.C.

[B70] Wooden, Wesley E., and Conover, Donald W. Human Engineering Guide for Equipment Designers, 1964. University of California Press, 1964.

[B71] Sheridan, Thomas B., and Ferrell, William R. Man-Machine Systems—Information, Control and Decision Models of Human Performance. MIT Press, 1974.

[B72] Karam, Douglas. Burn-In: Which Environmental Stress Screens Should be Used. RADC-TR-81-87, Mar 1981.

[B73] Bocchi, William J. Exponential Failure Distribution for Mechanical Reliability Prediction. RADC-TM-80-9, Dec 1980.

[B74] Reliability Predication of Electronic Equipment. Mil Hnbk-217D, Jan 1982.

[B75] Reliability Parts Derating Failures, RADC-TR-82-177. June 1982

[B76] A Study of Common Cause Failures. EPRI P-3383, Jan 1984 and EPRI NP-3837, June 1985.

[B77] IEEE Std 500-1984, IEEE Guide to the Collection and Presentation of Electrical, Electronic, Sensing Component and Mechanical Equipment Reliability Data for Nuclear Power Generating Stations. (ANSI)

Copyright © 1991 IEEE All Rights Reserved

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS Not for Resale

[B78] Enhancing Fossil Power Plant Design, Operation and Maintenance: Human Factor Guidelines. EPRI CS-745, vols. 1–4, Oct 1984.

[B79] Human Engineering Design Guidelines for Maintainability. EPRI NP-4350, Dec 1985.

[B80] Klion, Jerome. *A Redundancy Notebook*. RADC-TR-77-287, Dec 1977.

[B81] Hecht, H., Hecht, M. Fault Tolerance, Reliability and Testability for Distributed Systems. RADC-TR-83-36, Feb 1983.

[B82] Systematic Human Action Reliability Procedure (SHARP). EPRI NP-3583, Project 2170-3, June 1984.

[B83] IEEE 7432-1982, IEEE Application Criteria for Programmable Digital Computer Systems in Safety Systems of Nuclear Power Generating Stations. (ANSI, ANS)

[B84] *The Theory and Practice of Reliable System Design.* Digital Press, 1982.

[B85] IEEE 806-1986, IEEE Recommended Practice for System Identification in Fossil-Fueled Power Plants and Related Facilities.

Copyright © 1991 IEEE All Rights Reserved

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS Not for Resale

Annex A Reliability and Availability

(Informative)

A1 Definitions

Reliability: May be expressed either as failure rate (usual unit is 1/hour) or as mean time between failure (MTBF) (usually it is in hours). The relation between λ and MTBF depends on the evolution of λ versus time.

MTBF = $1/\lambda$ hours.

Mean Time to Repair (MTTR): The elapsed time to repair a component or a system after a fault has been detected. Replacing electronic modules is considered as repair in the above-mentioned sense.

The usual unit of MTTR is hours. The value of the MTTR depends on:

1) Quality of the fault identification feature provided with the control system.
2) Serviceability of the control system
3) Quality of the service personnel
4) Spare part policy of the user

NOTE — Keep MTTR as short as possible; for example, 15 minutes

Mean Time to Detection (MTM): The elapsed time between the occurrence of a failure until it is detected by the service personnel.

The MTTD depends on the technique used for the control system and on the quality of the fault detection system.

Outage Time (OT): The accumulation of MTTD and MTTR. During this time, the control system is not available to perform its function.

Availability (A): The ratio between that time during which the system is able to perform its duty and the total of this time and the outage time. The availability figure is a value between 0 and 1.

Unavailability (U): The ratio between the outage time and to the total outage time and the time during which the system performs its duty. The unavailability figure is a value between 0 and 1, and equals (1-A). (See Fig A1.)

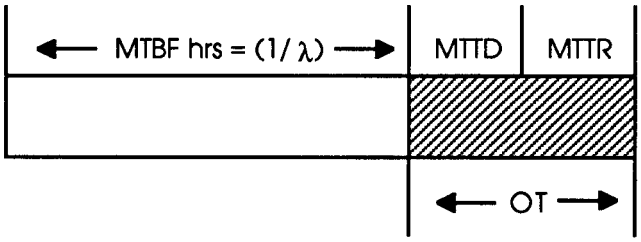
Failure Mode Effect Analysis (FMEA): Systematic process aimed at identification and elimination or compensation of failure modes for reliability improvement. This methodology is usually based on single failures.

Fault Tree Analysis (FTA): Systematic process involving a logic diagram that describes what combination of component (module) failures will cause a top event to occur.

Common mode failure source: An element of the control system that, when it fails, influences more than one piece of process-equipment, and inhibits operation of more than one out of a group of redundant process parts. Fault tree analysis assists in determining common mode failures, redundancy, etc.

Copyright © 1991 IEEE All Rights Reserved

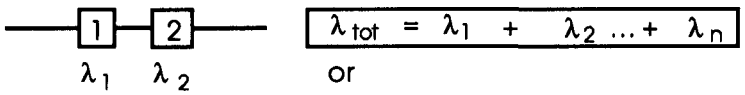
Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS Not for Resale



$$A = \frac{MTBF}{MTBF + MTTD + MTTR} = 1 - \frac{MTTD + MTTR}{MTBF + MTTD + MTTR}$$

$$U = 1 - \frac{MTBF}{MTBF + MTTD + MTTR}$$

Figure A1 —Unavailability



$$MTBF_{tot} = \frac{1}{\frac{1}{MTBF_1} + \frac{1}{MTBF_2} \cdots + \frac{1}{MTBF_n}}$$

Example: $\lambda_1 = 10^{-3}$ 1/h
$\lambda_2 = 10^{-4}$ 1/h
$\lambda_{tot} = 1.1 \cdot 10^{-3}$ 1/h ⟶ $MTBF_{tot}$ 900 hrs.

Figure A2 —Serial Structure

Common mode failure sources within the control system degrade the availability and in many cases the safety of a power plant see [B76] .

A2 Basic Calculations of System Reliability and Availability

An adequate reliability program for distributed control and monitoring systems should consist of qualitative and quantitative techniques. In terms of priorities, a qualitative FMEA and FTA should be implemented first and be supplemented by reliability and availability calculations.

Simple and summarized calculations can help considerably to make proper decisions regarding structure and required redundancy in a control system.

The following basic theory enables any engineer to make such simple evaluations. The reader is highly encouraged to read Appendix A, which includes detailed example problems. The examples chosen provide guidance for engineers to make their own simplified evaluation of different control structures regarding reliability and availability. Of main interest is always the total reliability of the combination plant/control. In addition, there are examples of common mode failures of redundant systems.

A3 Fundamental Theory

To calculate system reliability, the system structure has first to be analyzed.

Copyright © 1991 IEEE All Rights Reserved

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS Not for Resale

A3.1 Serial Structure

For components acting in series, the individual failure rates have to be added. (See Fig A2.)

From the formula given in Fig A2, it follows that the reliability of the worst component in a serial structure is predominant.

Or in other words, selecting reliable components in a serial structure cannot considerably improve system reliability if one or more weak components is included. The more components in series, the lower the over-all system reliability. That is one reason why it is suggested to utilize an integrated system approach instead of a segregated approach that may need many more components to operate properly.

A3.2 Parallel Structure

(See Fig A3.)

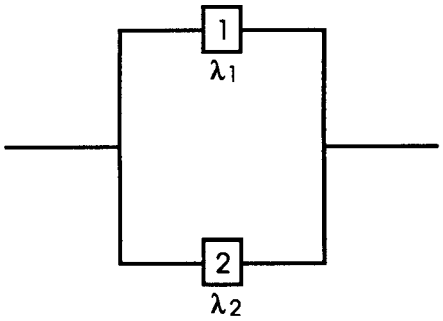
The formula given in Fig A3 shows that in parallel structures, the best component is predominate.

Although the probability for a component failure to occur is the same in both examples (i.e., the same number of spare parts is required within a certain period), the parallel structure will perform the system duty with a higher probability. FMEA and FTA can be utilized to justify critical and expensive spare parts at the power plant site instead of a central location for spare parts.

An even better performance of a parallel structure can be expected, if fault detection features are added and the faulty component is repairable (i.e., replaceable by a spare part) during normal service of the system. This is known as dynamic maintenance or hot repair.

In this case the system-function will only fail if the second component fails during the repair interval of the first. By this fault-detection and repair facility the failure rate λ of the system will be reduced. The formula to be used for this case is

$$\lambda_{tot} = 2 \cdot \lambda_1 \cdot \lambda_2 \cdot (MTTR + MTTD)$$



$$\frac{1}{\lambda_{tot}} = \frac{1}{\lambda_1} + \frac{1}{\lambda_2} - \frac{1}{\lambda_1 + \lambda_2}$$

Example: $\lambda_1 = 10^{-3}$ 1/h

$\lambda_2 = 10^{-4}$ 1/h

$$\frac{1}{\lambda_{tot}} = \frac{1}{10^{-3}} + \frac{1}{10^{-4}} - \frac{1}{10^{-3} + 10^{-4}} = 10090$$

$\lambda_{tot} = 0.99 \cdot 10^{-4}$ 1/h

or MTBF = 10090 hours ~ 1 year

Figure A3 —Parallel Structure

Copyright © 1991 IEEE All Rights Reserved

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS Not for Resale

where MTTR + MTTD is the total elapsed time between the occurrence of the fault and the commissioning of the spare part. It is suggested that critical spare parts be located at the power plant site to keep the MTTR as small as possible.

Assuming a total time of one hour for detection and repair of a fault and using the same λ values as before, the failure rate of the repairable system becomes:

$$\lambda_R = 2 \cdot 10^{-3} \cdot 10^{-4} \cdot 1 = 2 \cdot 10^{-7}\ 1/\text{h}$$

or

$$\text{MTBF}_R = \frac{1}{\lambda_R} = 0.5 \cdot 10^{+7}\ \text{hours} \sim 570\ \text{hours}$$

This typical example shows that extremely high reliability can be achieved by *repair facilities during operation of the system*, even when using components with moderate reliability.

It must be stressed, that nothing can be gained on reliability if the system has to be shut down for repair.

In the evaluation of control systems that utilize triple redundancy and two out of three failure logic, the Markov Chain approach for calculations may be utilized.

A4 Reliability and Availability—Power Plant Example

The three examples chosen provide guidance for engineers to make their own simplified evaluation of different control structures regarding reliability and availability. Of main interest is always the total reliability of the combination plant/control. In addition, an example of typical common mode failures of redundant system is included.

Failure rate value (λ) for components shall be taken from literature, vendor catalogs, or from experience. For examples of data sources see [B74] , [B75] , and [B77] . Care should be utilized when implementing these data sources. Failure rate data is extremely sensitive to temperature effects, make sure all failure rate data is taken at the same temperature. Also make sure that the vendor supplies the derating criteria of their components. Derating components is the key factor in assuring a high reliability of a distributed control and monitoring system.

The example chosen is an essential fluid supply service by two redundant pumps. An independent power supply to each pump is assumed for all solutions. Please note human reliability numbers are not included.

Three different solutions for the control of the two pumps will be analyzed.

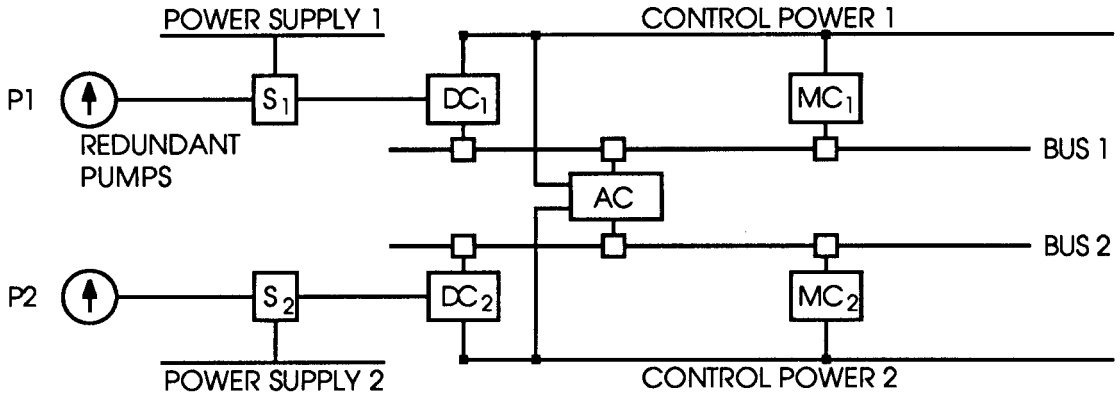
A4.1 Solution 1

A fully distributed control system as per Fig A4 is used. Two independent buses provide the data transmission.

Repair facilities during operation is assumed for all decentralized equipment. Power supplies to the control system are also distributed.

Copyright © 1991 IEEE All Rights Reserved

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS Not for Resale



P1/P2 Two redundant pumps. Operation of one pump is essential to maintain plant operation.
$\lambda_P = 10^{-5}$ 1/h
S1/S2 Switchgear $\lambda_S = 2 \cdot 10^{-6}$ 1/h
The corresponding power supplies are independent.
$\lambda_{PS} = 10^{-6}$ 1/h
DC_1/DC_2 Individual drive controller
$\lambda_D = 29 \cdot 10^{-6}$ 1/h
Control power supplies are independent.
$\lambda_{CP} = 10^{-6}$ 1/h
AC Automatic controls, common to P1/P2.
$\lambda_A = 29 \cdot 10^{-6}$ 1/h
MC Manual control station, individual for each drive.
$\lambda_M = 34 \cdot 10^{-6}$ 1/h
Bus1/Bus2 Two independent buses, linking DC, AC, MC.
$\lambda_B = 20 \cdot 10^{-6}$ 1/h

Figure A4 —Failure Rate Redundant Two-Pump System

A4.1.1 Plant Availability with Manual Control

This is the probability that fluid is supplied by at least one pump, using manual control.

Each of the two chains has a serial structure. Therefore,

$$\lambda_{tot1} = \lambda_{tot2} = \lambda_P + \lambda_S + \lambda_{PS} + \lambda_D + \lambda_{CP} + \lambda_B + \lambda_M$$

$$\lambda_{tot1} = \lambda_{tot2} = 9.7 \cdot 10^{-5} \text{ 1/h}$$

The two chains form together a parallel structure. Without repairs during operation results:

$$\frac{1}{\lambda_{tot}} = \frac{1}{\lambda_{tot_1}} + \frac{1}{\lambda_{tot_2}} - \frac{1}{\lambda_{tot_1} + \lambda_{tot_2}}$$

$$\lambda_{tot} = 6.47 \cdot 10^{-5} \text{ 1/h}$$

or

MTBF = 1.8 years

Copyright © 1991 IEEE All Rights Reserved

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS
Not for Resale

With repair facilities, the result is, of course, much better:

$$\lambda_{tot_R} = 2 \cdot \lambda_{tot_1} \cdot \lambda_{tot_2} \cdot (MTTD + MTTR)$$

Again assuming 1 hour for detection and repair:

$$\lambda_{tot_R} = 1.88 \cdot 10^{-8} 1/h$$

or

$MTBF_R = 53.14 \cdot 10^{+6}$ hours

$MTBF_R = 6066$ years

The availability of service will be

$$A = 1 - \frac{MTTD + MTTR}{MTBF + MTTD + MTTR} = 1 - 1.88 \cdot 10^{-8}$$

$A = 0.999999981$

if the system can be repaired during operation.

A4.1.2 Plant Availability With Automatic Control

This is the probability that fluid is supplied by at least one of the two pumps under full automatic control.

This case is only of interest if manual control is not feasible, because process reaction is too fast or extreme accuracy of flow has to be maintained. Only for some cases in a power plant do we have to face the problem, such as safety applications; for example, a turbine dc lube oil pump.

For automatic control we now have two serial structures working in parallel, and this combination works in series with the automation circuit:

$$\lambda_{tot_1} = \lambda_{tot_2} = \lambda_P + \lambda_S + \lambda_{PS} + \lambda_{CP} + \lambda_B = 63 \cdot 10^{-6} 1/h$$

Both lines in parallel and having repair-facilities yield:

$$\lambda_{tot_{1/2R}} = 2 \cdot \lambda_{tot_1} \cdot \lambda_{tot_2} \cdot (MTTD + MTTR)$$

$\lambda_{tot_1} = \lambda_{tot_2}$ has been calculated above and equals 63 · 10–6 1/h.

MTTD + MTTR is again assumed to be 1 hour, then we calculate:

$$\lambda_{tot_{1/2R}} = 2.63^2 \cdot 10^{-12} \cdot 1 = 7.938 \cdot 10^{-9}$$

Now we have to add the automation part, which has no repair-facility, as it is not redundant. The power supply to AC must be considered, as it is redundant and included in $\lambda_{tot_{1/2R}}$

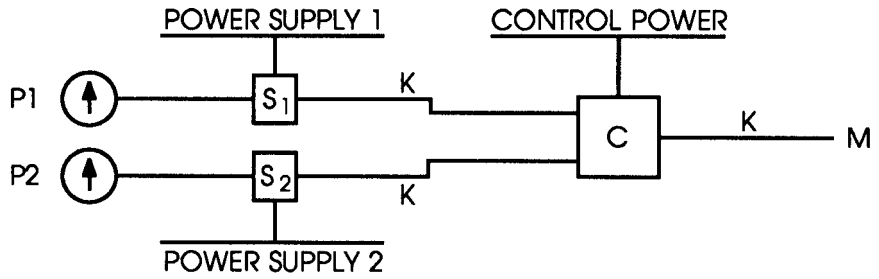
$$\lambda_{tot_R} = \lambda_{tot_{1/2R}} + \lambda_A = 29.007 \cdot 10^{-6} 1/h$$

or

$MTBF_R = 34{,}473$ hours = 3.93 years

Copyright © 1991 IEEE All Rights Reserved

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS Not for Resale



P_1/P_2, S_1/S_2 are as in A4.1, Solution 1.

C A controller of the same complexity as *AC* in A4.1, Solution 1.
$\lambda_C = 34 \cdot 10^{-6}$ 1/h

K Cable connections
$\lambda_K = 0.2 \cdot 10^{-6}$ 1/h

M Four (4) switches only, no electronics
$\lambda_M = 2 \cdot 10^{-6}$ 1/h

Figure A5 —Redundant Pumps With Centralized Controller

Such a figure might be at the limit of acceptance if manual back-up is not possible.

A4.1.3 Number of Spare Parts Used

For this calculation we have to add all λ values of all components in the system:

$\lambda_{tot} = 2 \cdot (\lambda_P + \lambda_S + \lambda_{PS} + \lambda_D + \lambda_{CP} + \lambda_B + \lambda_M) +$
$\lambda_A = 2.23 \cdot 10\text{-}4$ 1/h

or in MTBF = 4484 hrs ≅ 6 months; i.e., one has to expect a repair once every 6 months.

This figure helps to evaluate maintenance costs. Also keep in mind that failure mode effect analysis and fault tree analysis contributed to determining spare parts.

A4.1.4 Summing Up the Results for Solution 1

1) One repair per 6 months has to be expected for the complete system including pumps and switchgear.
2) Only once within 6,000 years a total loss of control over this fluid pumping system has to be expected, assuming the operation can be maintained with manual control. When automatic control goes to manual that should be considered a failure.
3) Once in 3.93 years, automatic control of the system will be lost.
4) If faults in the system are not repaired, manual control of the system would be lost once within 1.8 years.

A4.2 Solution 2

(See Fig A5.) The two pumps with individual power supplies are controlled by centralized control. Manual control acts via cable connection through the controller. No remote bus system is used.

A4.2.1 Plant Availability with Manual Control

This is the probability, that plant operation with at least one of the two pumps may be maintained, using manual control only.

Parallel part:

Copyright © 1991 IEEE All Rights Reserved

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS
Not for Resale

$$\lambda_{\text{tot}_1} = \lambda_P + \lambda_S + \lambda_{PS} + \lambda_K = \lambda_{tot_2} = 13.2 \cdot 10^{-6} 1/\text{h}$$

$$\frac{1}{\lambda_{\text{tot}_P}} + \frac{1}{\lambda_{\text{tot}_2}} - \frac{1}{\lambda_{\text{tot}_1} + \lambda_{\text{tot}_2}}$$

$$\lambda_{\text{tot}_p} = 8.8 \cdot 10^{-6} 1/\text{h}$$

Serial part:

$$\lambda_{\text{tot}_S} = \lambda_{CP} + \lambda_P + \lambda_K + \lambda_M = 37.2 \cdot 10^{-6} 1/\text{h}$$

Complete system:

$$\lambda_{\text{tot}} = \lambda_{\text{tot}_p} + \lambda_{\text{tot}_S} = 46 \cdot 10^{-6} 1/\text{h}$$

without repair.

We again assume repair-facilities for the portion with parallel structure.

$$\lambda_{\text{tot}_p} = 2 \cdot \lambda_{\text{tot}_1} \cdot \lambda_{\text{tot}_2} (\text{MTTD} + \text{MTTR})$$

$$\lambda_{\text{tot}_p} = 3.485 \cdot 10^{-10} 1/\text{h}$$

$$\lambda_{\text{tot}_R} = \lambda_{\text{tot}_p} + \lambda_{\text{tot}_S}$$

$$\lambda_{\text{tot}_p} = 37.2 \cdot 10^{-6} 1/\text{h}$$

or MTBF_R = 26881 hours ≅ 3.06 years with repair capability.

The availability of the fluid pumping service will be:

$$A = 1 - \frac{\text{MTTD} + \text{MTTR}}{\text{MTBF} + \text{MTTD} + \text{MTTR}} = 1 - 37 \cdot 10^{-6}$$

A = 0.9999628

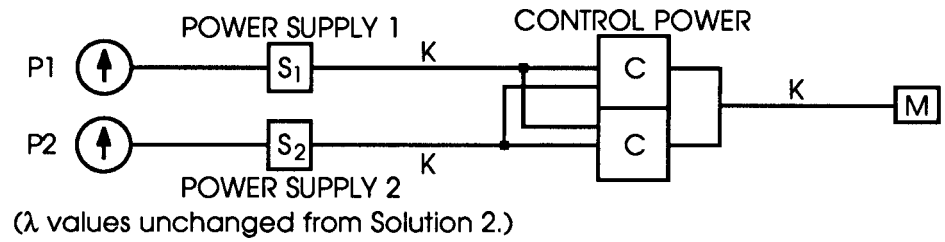


Figure A6 —Redundant Pumps with Redundant Controller

A4.2.2 Plant Availability with Automatic Control

This is the probability that plant operation can be maintained under automatic control.

The parallel part of the system remains unchanged compared to manual control.

Copyright © 1991 IEEE All Rights Reserved

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS Not for Resale

$$\lambda_{tot_p} = 3.485 \cdot 10^{-10} 1/h$$

The serial part is reduced to:

$$\lambda_{tot_S} = \lambda_{CP} + \lambda_C = 35 \cdot 10^{-6} 1/h$$

$$\lambda_{tot_R} = 3.485 \cdot 10^{-10} + 35 \cdot 10^{-6} \cong 35 \cdot 10^{-6}$$

$MTBF_R$ = 28,571 hours ≅ 3.26 years.

A4.2.3 Number of Spare Parts Used

Adding up λ values of all components results in:

$$\lambda_{tot} = 2 \cdot \lambda_P + \lambda_S + \lambda_{PS} + \lambda_K) + \lambda_C + \lambda_K + \lambda_M + \lambda_{CP}$$

$$\lambda_{tot} = 63.6 \cdot 10^{-6} 1/h$$

or

MTBF = 15 723 hours ≅ 1.8 years

A4.2.4 Summing Up the Results for Solution 2

1) One repair every 1.8 years has to be expected.
2) Once within 3 years, manual control over the system will be lost.
3) Once within 3.26 years, all control (auto and manual) will be lost.

Such a result may hardly be accepted for an essential service in a power plant. The most promising improvement would be to provide redundancy for the automatic controller. This case will be treated next as Solution 3.

A4.3 Solution 3

Solution 2 is improved by adding a redundant controller. (See Fig A6.)

A4.3.1 Plant Availability with Manual Control

First we calculate the two serial chains connected in parallel:

$$\lambda_{tot_1} = \lambda_{tot_2} = \lambda_P + \lambda_S + \lambda_{PS} + \lambda_K = 13.2 \cdot 10^{-6} 1/h$$

with repair facility:

$$\lambda_{tot_P} = 2 \cdot \lambda_{tot_1} \cdot \lambda_{tot_2} \cdot (MTTD + MTTR)$$

$$\lambda_{tot_P} = 3.485 \cdot 10^{-10} 1/h$$

The controllers have a parallel structure and can be repaired.

$$\lambda_{tot_C} = 2 \cdot \lambda_C \cdot \lambda_C \cdot (MTTD + MTTR)$$

$$\lambda_{tot_C} = 2.312 \cdot 10^{-9} 1/h$$

Copyright © 1991 IEEE All Rights Reserved

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS Not for Resale

The two parallel structures form a serial chain, which has to be extended with the power supply for the controllers and the manual control.

$$\lambda_{tot_R} = \lambda_{tot_P} + \lambda_{tot_C} + \lambda_{tot_{CP}} + \lambda_K + \lambda_M$$

$$\lambda_{tot_R} = 3.2 \cdot 10^{-6} 1/h$$

or

$$MTBF_R = 312240 \text{ hours} \cong 35.6 \text{ years}$$

$$A = 0.99999679$$

A4.3.2 Plant Availability with Automatic Control

Compared to the calculation for manual control K and M must be taken out.

$$\lambda_{tot_R} = \lambda_{tot_P} + \lambda_{tot_C} + \lambda_{CP}$$

$$\lambda_{tot_R} = 10^{-6} 1/h$$

or

$$MTBF_R = 1\ 000\ 000 \text{ hours} \cong 114 \text{ years}$$

In this case manual control is also lost.

A4.3.3 Number of Spare Parts Used

$$\lambda_{tot} = 2 \cdot (\lambda_P + \lambda_S + \lambda_{PS} + \lambda_K + \lambda_C) + \lambda_K + \lambda_{CP} + \lambda_M$$

$$\lambda_{tot} = 97.6 \cdot 10^{-6} \text{ 1/h}$$

or

$$MTBF = 10\ 245 \text{ hours} \cong 1.16 \text{ years}$$

A4.3.4 Summing Up Results for Solution 3

1) One repair within 1.16 years has to be expected.
2) Once within 35.6 years, manual control over the system will be lost.
3) Once within 114 years, all control (manual and auto) over the system will be lost.
4) If faults are not repaired the MTBF will be reduced to 3.62 years.

A4.4 Discussion of Results for Solutions 1, 2, and 3

The fully distributed Solution 1, if manual operation is feasible, yields the best solution because loss of total control, and therefore failure of the fluid supply, will occur only once within 6,000 years.

This solution is also very transparent and simple, but it needs the highest maintenance of the three solutions. As connecting cables are replaced by a remote bus, this solution might be cheaper than Solutions 2 and 3.

Solution 2 may only be acceptable for services that, when failing, will not trip a whole unit. The controller is predominant and responsible for the result. It is a centralized control.

Copyright © 1991 IEEE All Rights Reserved

--`,,`-`-`,,`,,`,`,,`---

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS Not for Resale

Solution 3 shows a considerable improvement compared to Solution 2. Automatic operation is now more reliable than manual operation, and also more reliable than automation in Solution 1. But this solution lacks the extremely reliable manual back-up provided by Solution 1. As the AC-function is redundant and all signals are transmitted by cables, Solution 3 is probably more expensive than Solution 1.

A number of common fault sources may be contained in the set-up shown in Fig A7 of two redundant PLCs or microprocessors:

1) The switch-over logic is inoperative.
2) The actual switch is mechanically or electrically deficient.

Such faults can be eliminated with consideration of the following:

1) Using a live zero fault signalling circuit will be helpful, but still does not exclude the possibility of a missing change-over signal.
2) Making the switch-over logic redundant, improves the reliability, but still does not exclude a single failure causing lack of switch-over.
3) Provide redundant switches.

A better way, however, is to give each PLC or microprocessor a sensing circuit that disables its own output as long as the redundant equipment works. (See Fig A8.)

With such a set-up, no fault in one of the two redundancies can prevent the other from working.

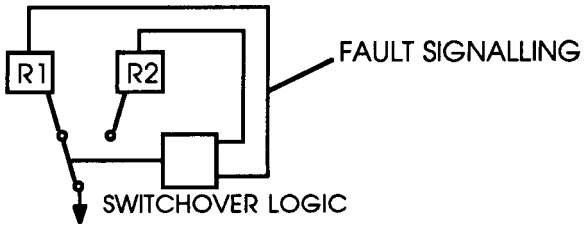


Figure A7 —Common Mode Failures of Redundant Systems

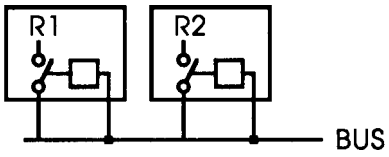


Figure A8 —Alternate Redundant Arrangement

Copyright © 1991 IEEE All Rights Reserved

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS Not for Resale

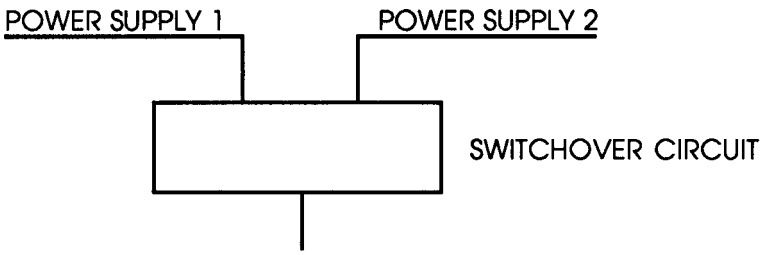


Figure A9 —Common Mode Failures of Redundant Systems

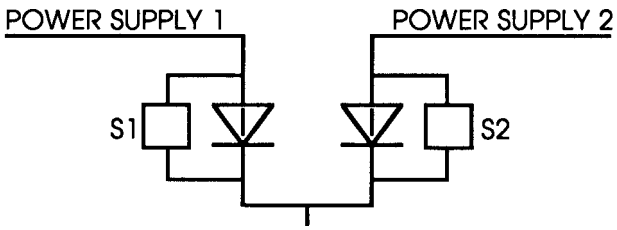


Figure A10 —Alternate Redundant Arrangement

One single fault in the switch-over circuit can prevent switchover, as shown in Fig A9.

The alternative solution shown in Fig A10 will properly fulfil the one fault criteria. To prevent a second fault before the first is repaired, it is essential that diode failures are detected by alarms S1 and S2.

Copyright © 1991 IEEE All Rights Reserved
--`,,-`-`,,`,,`,`,,`---

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS
Not for Resale

Annex B FMEA/FTA Failure Mode Effect Analysis (FMEA)

(Informative)

The failure analysis of a control system is accomplished by a qualitative analysis approach called failure mode effect analysis (FMEA). This approach was developed by safety and reliability engineers so that problems arising from equipment failures could be easily identified.

The primary objective of the FMEA is to determine ways to eliminate or reduce the possibility of critical failure modes and improve the control system design. The suggested format to utilize is shown in Fig B1. This approach will illustrate the critical failure as well as providing a preventive measure with a low cost.

Each component(s) can be analyzed using this format. The FMEA not only indicates what effect a component (module) failure may have and how to prevent it, but also identifies critical components and what changes are most desirable to make first.

Figure B1 explains what should be placed in each column from one to ten. Refer to the top of the FMEA format entitled “Key to Column Code” just below the “Subsystem” block. Note, there is a list of items under column comparison of negligible effects to catastrophic effects with weighting factors of one to five. These are used in Column 5 entitled “Class.” Column 6 has a list of relative hazard numbers from unknown (1) to chronic, frequent occurrence (4). These weighting factors are put in Column 6 entitled Relative Hazard Number. Column 9, Cost Index, has weighting factors of one to four, one being the expensive preventive measure and four being the most economical.

Note, Column 7 is a Hazard Index Number. It is the resultant product of Column 5 (Class) and Column 6 (Relative Hazard Number). This number gives an indication of the criticality of the component (module). The higher this number, the more critical the component (module) failure is to the distributed control system.

Also, the Economical Guideline Index in Column 10 is an indication of what distributed control system changes are most desirable to make first. This index number is a product of Column 7 (Hazard Index Number) and Column 9 (Cost Index). The higher this index number as compared to another in this column is an indication that the failure is critical and can be eliminated economically or at a lower cost.

Copyright © 1991 IEEE All Rights Reserved

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS Not for Resale

SYSTEM:	SUBSYSTEM:	ENGINEER:	DATE:

KEY TO COLUMN CODE

COLUMN 5 - CLASS

1. NEGLIGIBLE EFFECT
2. MARGINAL REPAIRS REQ'D.
3. PARTIAL LOSS OF AVAILABILITY
4. LOSS OF UNIT AVAILABILITY
5. CATASTROPHE, LOSS OF LIFE, MAJOR ACCIDENT (EXPLOSION, IMPLOSION, ETC.)

COLUMN 6 - RELATIVE HAZARD NO.

1. UNKNOWN OR > 12 YRS. MTBF
2. RANDOM, INFREQUENT, 4-12 YRS. MTBF
3. OCCASIONAL OCCUR. 2-4 YRS. MTBF
4. CHRONIC, FREQUENT OCCURANCE 0-2 YEARS MTBF

COLUMN 9 - COST INDEX (MULTIPLY BY 1,000)

1. 10-20
2. 5-10
3. 1-5
4. LESS THAN 1

COL 1	COL 2	COL 3	COL 4	COL 5	COL 6	COL 7	COL 8	COL 9	COL 10
COMPONENT (MODULE)	FAILURE MODE	CAUSE	EFFECT	CLASS	RELATIVE HAZARD NO.	HAZARD INDEX # COL. 5 X COL. 6	PREVEN-TIVE MEASURES	COST INDEX	ECONOMICAL GUIDELINE COL. 7 X COL. 9
FILL OUT ONE SHEET FOR EACH SUBSYSTEM OR COMPONENT (MODULE). IN THIS COLUMN LIST EACH WAY THAT THE BOARD CAN FAIL DUE TO NORMAL USE, ABNORMAL USE (WITH OR WITHOUT AIR CONDITIONING) OR MISUSE.	COULD IT FAIL, NOT WILL IT FAIL.	CAUSE OF FAILURE MODE NOTED IN COLUMN 1.	IN THIS COLUMN TRY TO THINK OF THE WORST POSSIBLE HAZARDOUS CONDITION OR RESULT THAT MIGHT OCCUR DUE TO EACH FAILURE MODE IN COLUMN 1.	ASSIGN A CLASS TO EACH EFFECT ACCORDING TO LIST AT THE TOP OF THIS FORM AND WRITE THE NUMBER IN THIS COLUMN.	BASED UPON VENDOR'S EXPERIENCE AND HISTORY OF PRODUCT, WRITE THE RELATIVE HAZARD NUMBER IN THIS COLUMN.	MULTIPLY COLUMN 5 AND 6 AND PUT RESULT IN THIS COLUMN. THIS NUMBER GIVES AN INDICATION OF THE CRITICALITY OF THE COMPONENT (MODULE).	FOR EACH HAZARD WITH A RELATIVELY HIGH HAZARD INDEX, WRITE DOWN AS MANY WAYS AS YOU CAN THINK OF TO AVOID THE EFFECT LISTED IN COLUMN 2.	FOR EACH MEASURE IN COLUMN 8, WRITE THE COST INDEX IN THIS COLUMN.	THIS COLUMN (INDEX) CAN BE UTILIZED AS A GUIDE IN SELECTING THE ORDER IN WHICH CHANGES ARE TO BE IMPLEMENTED.

Figure B1 —Suggested (FMEA) Format

Copyright © 1991 IEEE All Rights Reserved

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS Not for Resale

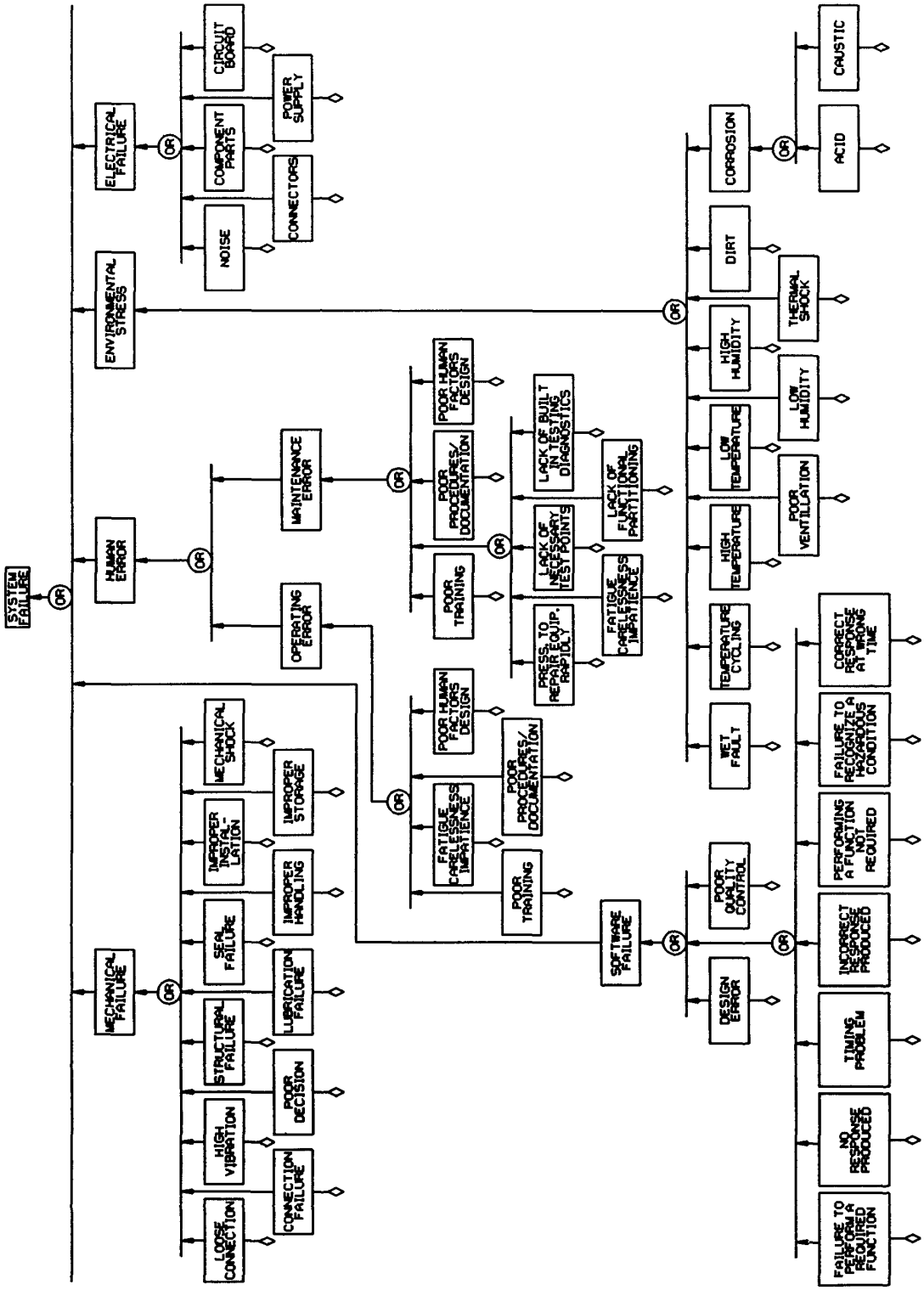


Figure B2 —Fault Tree for a System Failure

Copyright © 1991 IEEE All Rights Reserved

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS
Not for Resale