

WITHDRAWN

IEEE Std 1046™-1991(Withdrawn 2006)

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**

Withdrawn 3 February 2006
IEEE-SA Standards Board

**The Institute of Electrical and Electronics Engineers, Inc.
3 Park Avenue, New York, NY 10016-5997, 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.

* “Withdrawn” standards are standards that are no longer useful or contain significant obsolete or erroneous information. All amendments or corrigenda associated with this standard have also been withdrawn.

WARNING: You are cautioned to USE AT YOUR OWN RISK, as the technology contained herein may no longer be accurate, or may have been superseded since the date of withdrawal.
--

Information on withdrawn standards is available in the IEEE-SA Standards Board Operations Manual
<<http://standards.ieee.org/guides/opman/index.html>>.

WITHDRAWN

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 monitoring systems are addressed.

Keywords: Power plant, control, distributed control, digital, monitoring, distributed monitoring

WITHDRAWN

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.

WITHDRAWN

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

WITHDRAWN

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

WITHDRAWN

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

WITHDRAWN

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

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.)

WITHDRAWN

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

WITHDRAWN

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.

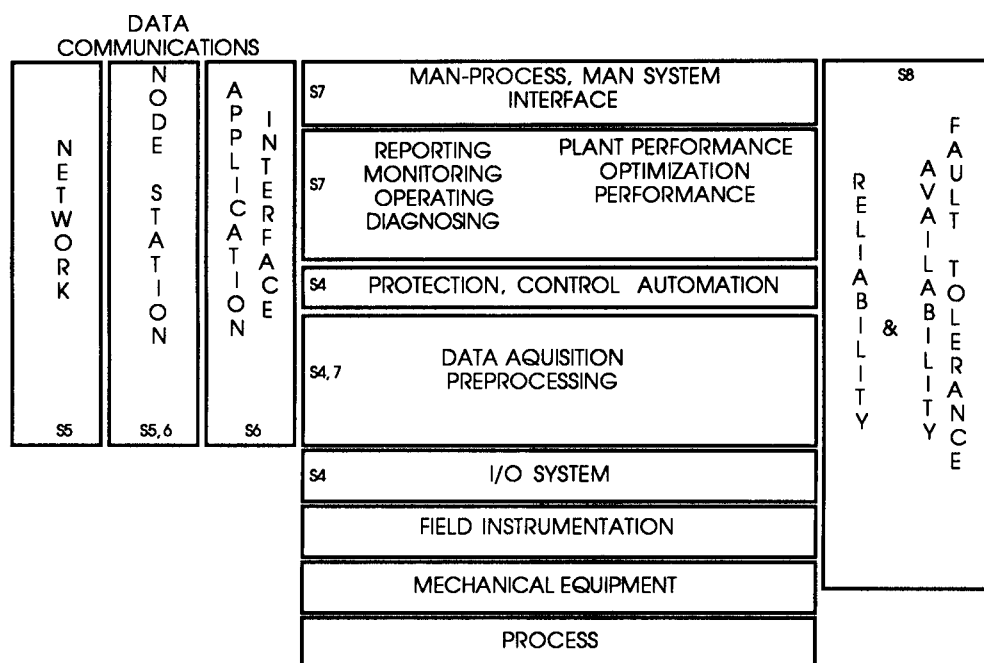


Figure 1—Architectural View of IEEE Std 1046-1991

WITHDRAWN

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

WITHDRAWN

- 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 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.

WITHDRAWN

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 functionality 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

WITHDRAWN

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 peripheral 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.

WITHDRAWN

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.

WITHDRAWN

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.

WITHDRAWN

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.

WITHDRAWN

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.

WITHDRAWN

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:

WITHDRAWN

- 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

WITHDRAWN

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.

WITHDRAWN

- 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.

WITHDRAWN

- 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

WITHDRAWN

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.

WITHDRAWN

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.

WITHDRAWN

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.

WITHDRAWN

- 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.

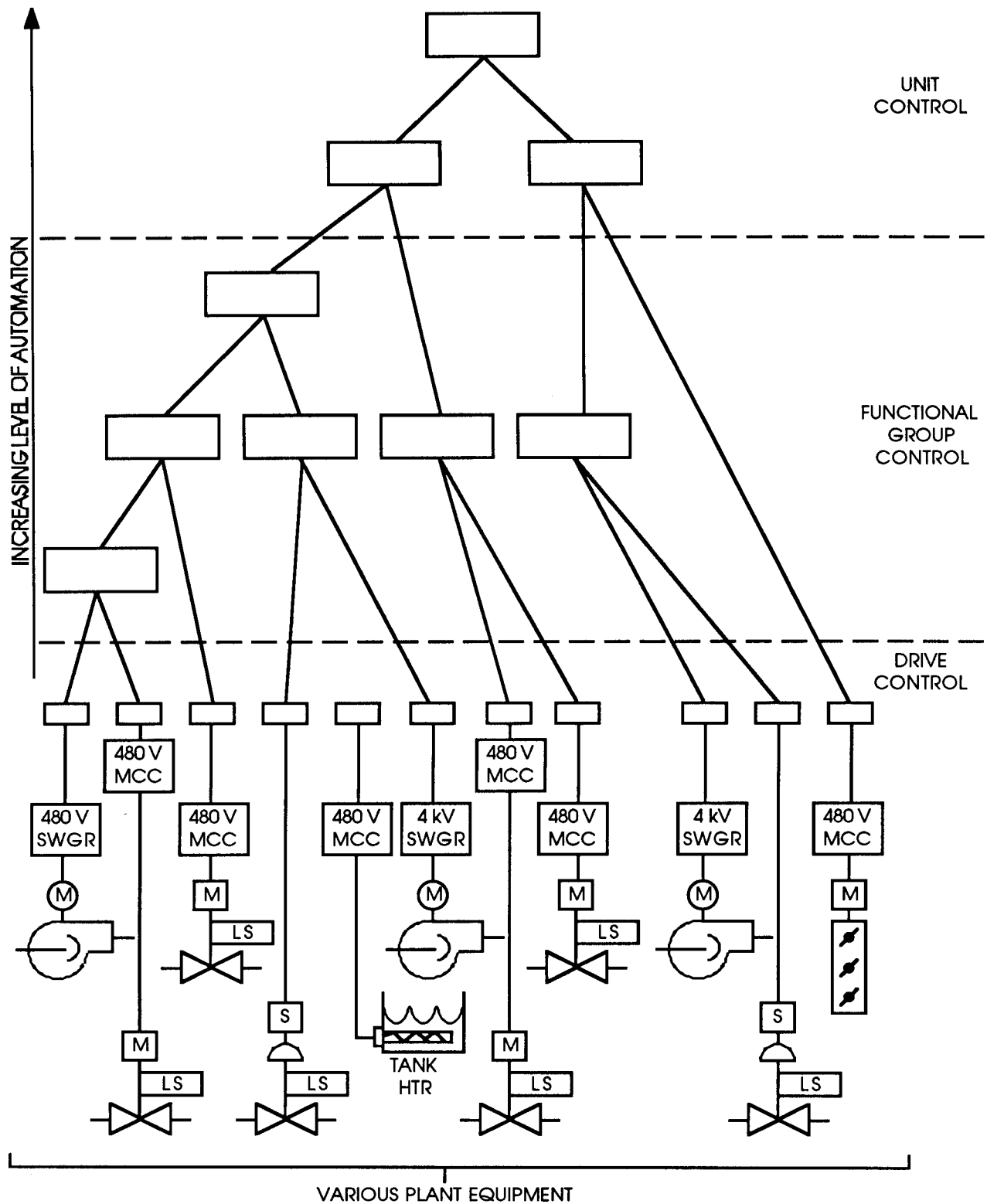


Figure 2—Hierarchical Structure

WITHDRAWN

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.

WITHDRAWN

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.

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

WITHDRAWN

- 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

WITHDRAWN

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.

WITHDRAWN

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:

WITHDRAWN

- 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.

WITHDRAWN

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:

WITHDRAWN

- 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 mA_{dc} 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 mA_{dc} 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