Process Control Systems—
Process Control System Design

API RECOMMENDED PRACTICE 554, PART 2
FIRST EDITION, OCTOBER 2008

Process Control Systems—
Process Control System Design

Downstream Segment

API RECOMMENDED PRACTICE 554, PART 2
FIRST EDITION, OCTOBER 2008

Special Notes

API publications necessarily address problems of a general nature. With respect to particular circumstances, local, state, and federal laws and regulations should be reviewed.

Neither API nor any of API's employees, subcontractors, consultants, committees, or other assignees make any warranty or representation, either express or implied, with respect to the accuracy, completeness, or usefulness of the information contained herein, or assume any liability or responsibility for any use, or the results of such use, of any information or process disclosed in this publication. Neither API nor any of API's employees, subcontractors, consultants, or other assignees represent that use of this publication would not infringe upon privately owned rights.

API publications may be used by anyone desiring to do so. Every effort has been made by the Institute to assure the accuracy and reliability of the data contained in them; however, the Institute makes no representation, warranty, or guarantee in connection with this publication and hereby expressly disclaims any liability or responsibility for loss or damage resulting from its use or for the violation of any authorities having jurisdiction with which this publication may conflict.

API publications are published to facilitate the broad availability of proven, sound engineering and operating practices. These publications are not intended to obviate the need for applying sound engineering judgment regarding when and where these publications should be utilized. The formulation and publication of API publications is not intended in any way to inhibit anyone from using any other practices.

Any manufacturer marking equipment or materials in conformance with the marking requirements of an API standard is solely responsible for complying with all the applicable requirements of that standard. API does not represent, warrant, or guarantee that such products do in fact conform to the applicable API standard.

Foreword

Nothing contained in any API publication is to be construed as granting any right, by implication or otherwise, for the manufacture, sale, or use of any method, apparatus, or product covered by letters patent. Neither should anything contained in the publication be construed as insuring anyone against liability for infringement of letters patent.

Shall: As used in a standard, “shall” denotes a minimum requirement in order to conform to the specification.

Should: As used in a standard, “should” denotes a recommendation or that which is advised but not required in order to conform to the specification.

This document was produced under API standardization procedures that ensure appropriate notification and participation in the developmental process and is designated as an API standard. Questions concerning the interpretation of the content of this publication or comments and questions concerning the procedures under which this publication was developed should be directed in writing to the Director of Standards, American Petroleum Institute, 1220 L Street, N.W., Washington, D.C. 20005. Requests for permission to reproduce or translate all or any part of the material published herein should also be addressed to the director.

Generally, API standards are reviewed and revised, reaffirmed, or withdrawn at least every five years. A one-time extension of up to two years may be added to this review cycle. Status of the publication can be ascertained from the API Standards Department, telephone (202) 682-8000. A catalog of API publications and materials is published annually by API, 1220 L Street, N.W., Washington, D.C. 20005.

Suggested revisions are invited and should be submitted to the Standards Department, API, 1220 L Street, NW, Washington, D.C. 20005, standards@api.org.

Contents

Page

Figures

Tables

Introduction

Advances in computing and digital communications technologies since the preparation of the first edition of API 554 have had major impacts on the way instrumentation and control systems function as compared to historical designs. The advances have also radically changed the way that the design and specification of such systems must be approached and have created major issues relative to system design and system security. These issues are as follows.

— The virtual disappearance of conventional central control room control panels.

— Advances in computing power, software standards and communications standards have resulted in many of the functions historically implemented in stand alone process control and historization computers being integrated within the process control systems. This has greatly expanded the scope of process control system design and blurred the division between real time control and historization functions and higher-level information systems that provide input to business and maintenance systems.

— Advances in field instrumentation design leading to the general use of “smart” digital field instrumentation. Further advances in field bus and related technologies allow these “smart” instruments to communicate directly with the process control systems or with each other. These instruments not only transfer information about the basic process measurement, but also communicate diagnostic information about the health of the device or other secondary information derived from the primary measurements.

— Further developments in standardization of operating systems and software practices have enabled use of standard computer components and peripherals operating on standard operating systems. This has resulted in a developing trend away from control systems applications being implemented on proprietary hardware and software systems, but rather being implemented on standard personal computer, workstation and network communication products running widely available operating systems.

— This standardization has reduced the cost and increased the flexibility of the systems. It has also resulted in greater exposure of the process control system to external interference and requires additional support to keep the operating systems current and secure. Security and virus-protection are major concerns of newer process control systems and must be addressed at both the design and operational phases.

The result of all these technical advances is that process control systems are no longer entirely based upon proprietary closed hardware and software systems offered by a single vendor. While these implementations are still available and form the preponderance of the existing installed base, there is a very strong trend away from closed systems provided by one vendor, to more open systems based upon industry standard hardware and software which have both proprietary and open system components.

These trends result in a far greater flexibility in selection of the control functions and the control hardware.

These trends place greater responsibility upon the design engineer and user to understand the interaction between process control systems and the business functions of an organization; select and specify the functions that are necessary for a given application; and implement those functions in a safe, reliable, cost effective and maintainable manner.

Therefore, this edition of API 554 has been reorganized and split into three documents in order to better define the processes required to properly scope, specify, select, install, commission, operate, and maintain process control systems. This recommended practice is not intended to be used as a purchase specification, but recommendations are made for minimum requirements that can be used as a specification basis.

Process Control Systems—Process Control System Design

1 Scope

This recommended practice (RP) addresses the processes required to successfully implement process control systems for refinery and petrochemical services. The major topics addressed are listed below.

— *Part 1*. The basic functions that a process control system may need to perform, and recommended methodologies for determining the functional and integration requirements for a particular application.

— *Part 2*. Practices to select and design the installation for hardware and software required to meet the functional and integration requirements.

— *Part 3*. Project organization, skills and management required to execute a process control project and then to own and operate a process control system.

Figure 1 shows the general overall scope of refinery control and automation functions and the portions of which this recommended practice addresses.

The first edtions of API 554, Part 2 and API 554, Part 3 have been prepared by a collaborative effort of the API Subcommittee on Instrumentation and Control Systems and the PIP (Process Industries Practices) Process Control Function Team. As such, the general scope of the material contained has been expanded to cover general industrial process control topics that are applicable to both refineries and petrochemical facilities (PIP is a consortium of owner and engineering/construction contractor companies whose purpose is to produce a set of harmonized engineering standards in a variety of discipline areas, including process control).

Although the scope has been extended beyond traditional refining services, the user is cautioned to fully consider the requirements of the particular applications and circumstances that may exist and carefully apply the concepts described in this RP as appropriate. This document is not intended to present a tutorial on the subjects discussed, but rather to aid the reader in identifying and understanding the basic concepts of process control systems. The references provided within the document direct the reader to publications that describe one or more subjects in greater detail than is necessary or desirable for the purposes of this document.

1.1 Document Organization

This document is organized to follow the sequence of activities associated with the typical life cycle of a process control system as summarized in Table 1.

The life cycle phases as they apply to process control systems are listed below.

— *Appraise*. Develop business goals and requirements and identify basic functions required. This step is often also referred to as the conceptual stage.

— *Select*. Further develop business goals and functions into a process control systems scope definition. This step often is part of the early portion of front end engineering design (FEED).

— *Define*. Finalize process control systems scope definition, select hardware and software and prepare all applicable design drawings, specifications and procure other hardware and equipment. This step often forms the bulk of FEED.

— *Execute*. Detailed design and procurement, construction/installation, checkout, commissioning.

— *Operate*. Commission operate and maintain.

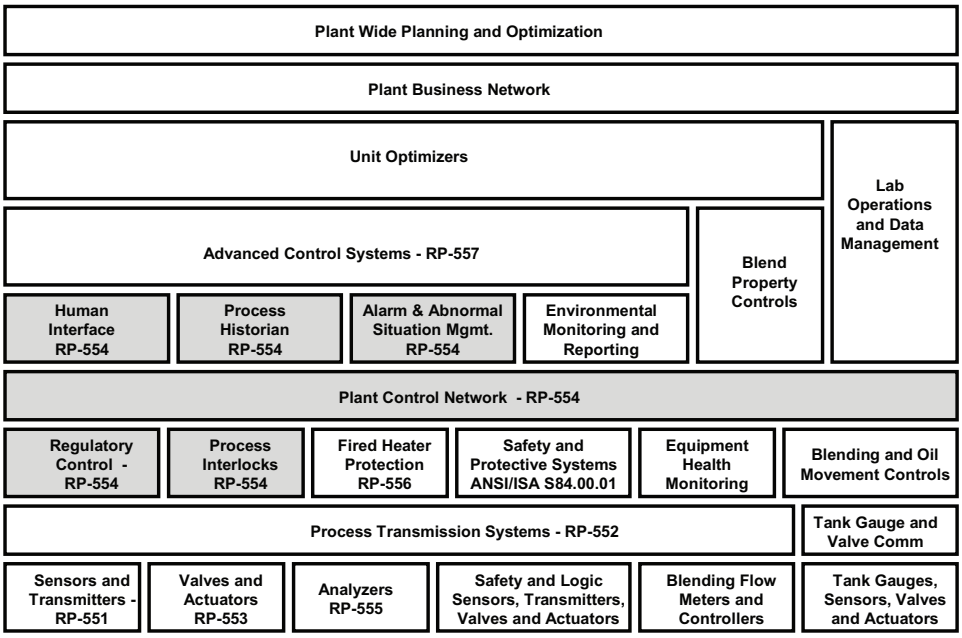

Figure 1—Refinery Control and Automation Functions

API 554 has been divided into three parts, each focusing on a major aspect of process control systems. The three parts and the areas that they cover are as follows.

— *Part 1, Process Control System Functions and Functional Specifications*. Covers the basic functions that a process control system may need to perform, and describes recommended methodologies for determining the functional and integration requirements for a particular application.

— *Part 2, Process Control System Design*. Covers the hardware and software applied to process control systems and provides recommendations for implementation. Design considerations and references to design practices for control centers and other control system buildings and enclosures are also provided.

— *Part 3, Process Control System Project Execution and Ownership*. Covers project organization, skills and work processes required to execute a process control project and then to own and operate a process control system.

The portions of API 554 that deal with each phase of the life cycle are identified in Table 1.

1.2 Part 2—Introduction

API 554, Part 1 describes the concepts involved in identifying and documenting functional requirements for process control systems. Part 2 is intended to address implementation of those process control systems functions using the hardware and software systems in general use at the time of publications. This portion of the RP will be subject to more frequent updates as the underlying control technologies change and mature.

Table 1—Process Control Systems Life Cycle Overview

API 554 Section Number	Phase	Objectives	Major Inputs	Major Outputs
Part 1, Sec. 2	Appraise/conceptual design	Document the business goals and basis for the project	Process design, PFDs, equipment list, existing systems and infrastructure, layout, business objectives, operations staffing plan, corporate master plan, control system standards	Process control system conceptual design basis
Part 1, Sec. 3, 4	Select/FEED	Develop a functional specification describing the scope of the project, functional requirements and overall implementation responsibilities	Design basis, P&IDs, equipment lists, process hazard analysis Process control system conceptual design basis	Process control system functional specification
Part 2	Define/execute (FEED/ detailed design)	Prepare request for quote, issue, and select a vendor Specify hardware, I/O layouts and communications Design control centers, field devices, interconnecting wiring, instrument power Define control systems interfaces to other systems and hardware	Process control system functional specification Design standards and practices Documentation requirements	Hardware and software selection. Detailed specifications and installation/construction drawings
Part 3	Execute—project execution and management	Execute designs to meet cost, schedule and technical requirements	Project objectives, cost and schedule	Complete design drawings and specifications. Procurement of all materials and equipment. Implementation and testing of all software based functions
Parts 2, 3	Execute—construction and installation	Install, calibrate, and loop test instrumentation and control systems	Design drawings and specifications. Configuration and programming. Equipment and systems manuals	Process control systems ready for operation
Part 3	Operate—commission	Prepare process controls system for operation	Performance requirements	Process control systems in operation. All deficiencies identified and corrected
Part 3	Operate—operation	Operate process control system to best operational effectiveness	Performance requirements	Business revenue and minimal costs
Part 3	Operate—maintain	Maintain, preventative maintenance (PM) and repair process control systems	As-built documentation and training	Maximum unit performance and availability

2 Referenced Publications

A number of publications are either directly referenced in the discussions in Part 1, Part 2 and Part 3 of API 554, or are part of general collection of standards and practices upon which process control systems are based. These are listed for reference. However, the user of a particular publication is responsible for identifying the applicability of any of the references to a particular installation. Local jurisdiction requirements may supplement or override the contents of any of these publications.

API Recommended Practice 551, *Process Measurement Instrumentation*

API Recommended Practice 552, *Transmission Systems*

API Recommended Practice 553, *Refinery Control Valves*

API Recommended Practice 555, *Process Analyzers*

API Recommended Practice 556, *Fired Heaters and Steam Generators*

API Recommended Practice 557, *Guide to Advanced Control Systems*

API Recommended Practice 750, *Management of Process Hazards*

AICHE 6-1212 [1], *Guidelines for Safe Automation of Chemical Processes*

AICHE G-66, *Layer of Protection Analysis: Simplified Process Risk Assessment*

AICHE *Guidelines for Safe and Reliable Instrumented Protective Systems*

EEMUA 191 [2], *Alarm Systems—A Guide to Design, Management and Procurement*

EEMUA 201, *Process Plant Control Desks Utilising Human-Computer Interfaces*

EIA RS-232C [3], *Interface Between Data Terminal Equipment and Data Communication Equipment Employing Serial Data Interchange*

TIA/EIA 422-B, *Electrical Characteristics of Unbalanced Voltage Digital Interface Circuits*

TIA/EIA RS 485, *Multi-point Electrical Characteristics of the Balanced Voltage Digital Interface Circuit*

IEC 61131-3 Parts 1 – 7 [4], *Programmable Controllers, Part 3, Programming Languages*

IEC 61158, *Digital Data Communications for Measurement and Control—Fieldbus for Use in Industrial Control Systems,*

IEC 61508 Parts 1 – 7, *Functional Safety of Electrical/Electronic/Programmable Electronic Safety Related Systems*,

IEC 61511 Parts 1 – 3, *Functional Safety Instrumented Systems for the Process Industry Sector*

---

1 American Institute of Chemical Engineers, Center for Chemical Process Safety, 3 Park Ave, New York, New York, 10016-5991, www.aiche.org/ccps/.

2 Engineering Equipment and Materials Users Association, 10-12 Covat Lane, London, EC3R8DN, United Kingdom, www.eemua.org.

3 Electronic Industries Alliance, 2500 Wilson Blvd., Arlington, Virginia 22201, www.eia.org.

4 International Electrotechnical Commission, 3, rue de Varembe, P.O Box 131, CH-121 Geneva 20, Switzerland, www.iec.ch.

IEC 61512 Parts 1 – 3 , *Batch Control*

IEEE Std 484–1996 [5], *Recommended practice for installation design and installation of vented lead-acid batteries for stationary applications*

IEEE Std 802.3–2005 Part 3, *Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications*

IEEE Std 802.11–2007, *Standard for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*

ISA 18.1 [6], *Annunciator Sequence and Specifications*

ISA S17.1, *Environmental Conditions for Process Measurement and Control*

ISA 84.00.01(IEC 61511 Mod), *Functional Safety: Safety Instrumented Systems for the Process Industry Sector*

ISA TR84.00.02-2002, *Safety Instrumented Functions (SIF) Safety Integrity Level (SIL) Evaluation Techniques, Part 1: Introduction*

ISA TR84.00.02-2002, *Safety Instrumented Functions (SIF) Safety Integrity Level (SIL) Evaluation Techniques, Part 2: Determining the SIL of a SIF via Simplified Equations*

ISA TR84.00.02-2002, *Safety Instrumented Functions (SIF) Safety Integrity Level (SIL) Evaluation Techniques, Part 3: Determining the SIL of a SIF via Tree Analysis*

ISA TR84.00.03-2002, *Guidance for Testing of Process Sector Safety IInstrumented Functions (SIF) Implemented as or Within Safety Instrumented Systems (SIS) Society*

ISA 88.01, *Batch Control Systems: Models and Terms*

ISA 91.00.01, *Identification of Emergency Shutdown Systems and Controls That Are Critical to Maintaining Safety in Process Industries*

ISA 95.00.01, *Enterprise-Control System Integration—Part 1: Models and Terminology*

ISA 98.00.01-2002, *Qualifications and Certification of Control System Technicians*

ISA TR98.00.02-2006, *Skill Standards for Control System Technicians*

ISA 99.00.01, *Security for Industrial Automation and Control Systems, Part 1: Models and Terminology*

ISA TR99.00.02, *Manufacturing Control Systems Security—Establishing Manufacturing and Control Systems Security Program*

ISA 99.00.03—*Operating a Manufacturing and Control Systems Security Program*

ISA 99.00.04, *Specific Security Requirements for Manufacturing and Control Systems*

---

5 Institute of Electrical and Electronics Engineers, 1828 L Street, N.W., Suite 1202, Washington, D.C. 20036-5104, www.ieee.org.

6 The Instrumentation, Systems, and Automation Society, 67 Alexander Drive, Research Triangle Park, North Carolina 27709, www.isa.org.

ISA SP100.11a, *Wireless Systems for Automation (Draft)*

ISA *Fieldbuses for Process Control: Engineering, Operation and Maintenance*

NFPA 70 [7], *National Electric Code*

NFPA 75, *Standard for the Protection of Electronic Computer/Data Processing Equipment*

NFPA Article 250, *Grounding*

NFPA Article 440, *Air-Conditioning and Refrigeration Equipment*

NFPA 493, *Intrinsically Safe Apparatus in Sivision I Hazardous Locations*

NFPA 496, *Purged and Pressurized Enclosures for Electrical Equipment*

NFPA 497A, *Fire Protection Handbook*

NFPA Article 500, *Hazardous (Classified) Locations*

NFPA 700-12(a), *Chapter 7—Emergency Systems Sub Section C. Sources of Power 700-12 General Requirement (a) Storage Battery*

OSH 29 *CFR* 1910 [8], *Code of Federal Regulations Title 29—Occupational Safety and Health Standards*

PIP PCEDO001 [9], *Guideline for Control System Documentation*

PIP PCCEL001, *Instrumentation Electrical Requirements*

PIP PCSCP001, *Procurement of Control Panels*

PIP STC01018, *Blast Resistant Design Criteria*

PIP ARS13120, *Pre-engineered Metal Buildings Specification*

3 Definitions

3.1
batch control
Refers to control functions that occur in a series of complex steps or phases that may combine continuous control, sequence control and discrete control to execute a processing scheme.

3.2
bridge
Refers to a communications network device that allows communications between network branches that use different communications media or protocols.

[7] National Fire Protection Association, 1 Batterymarch Park, Quincy, Massachusetts 02169-947, www.nfpa.org.
[8] Occupational Safety and Health Administration, U.S. Department of Labor, 200 Constitution Avenue, NW, Washington, D.C. 20210, www.osha.gov.
[9] Process Industry Practices, 3925 West Braker Lane (R4500), Austin, Texas 78759, www.pip.org.

3.3
business network
Refers to a digital communications network that is used for general purpose business use such as desktop computing, non-process control data base applications or other general purpose applications. Typically, business networks use industry standard communications methods such as ethernet.

3.4
continuous control
Refers to control functions that are continuously and repetitively executed to control the values of process variables such a pressure, temperature, flow, etc. that are part of a continuous process such as a refining process, or within a portion of a process associated with a batch control system.

3.5
control center
Refers to an inhabited facility (typically a building) which houses plant personnel and process control systems equipment to permit the operation and coordination of one or more process plants. Control centers are not always located adjacent to the process equipment being controlled and often centralize operation of multiple process plants or areas. Trends are to locate control centers away from potential blast zones.

3.6
control loop
Refers to that part of an instrument control system which includes the input sensor, transmitter, communication path, control algorithm and final control element. Control algorithm may be executed as one of many such algorithms in a process control system or be performed by stand alone electronic, pneumatic or mechanical devices.

3.7
control module
Refers to a processing module that performs various control and data acquisition functions in a process control system. Typically, this module is used to poll data from system I/O modules, perform basic regulatory or other control functions and communicate I/O and control information to other modules in the process control system.

3.8
demilitarized zone
DMZ
Refers to an additional digital communications network that is inserted between a network that is exposed to the internet and public use networks and a protected network. In practice relative to this RP, a DMZ is located between a business LAN and the process control network.

3.9
distributed control system
DCS
Refers to a general term used for digital process control systems that use multiple processing modules to perform the functional tasks of the system. These modules may or may not be located in physical proximity to one another.

3.10
discrete control
Refers to control functions that involve on-off operations and interlocks. Discrete control variables are generally associated with thresholds above or below which a control action is taken. The control action is a discrete function such as opening or closing a valve, starting or stopping a motor, etc.

3.11
electro-magnetic inference
EMI
Refers to electro-magnetic interference which may affect operation of electronic equipment due to electromagnetic fields generated by power wiring, motors or other electrical equipment.

3.12
encryption
Refers to the coding and decoding of data transmissions using algorithms and encryption keys that are known only to the sending and receiving devices. A wide variety of encryption techniques and algorithms are available and have varying levels of security associated with them.

3.13
enterprise resource planning
ERP
Refers to systems that are used to identify and coordinate supplies of raw materials, intermediate materials, finished products, consumables and other material or resources required to operate a manufacturing business.

3.14
ethernet
Refers to a networking standard that uses a single cable consisting of four pairs of wires to connect multiple computing devices together in a manner that does not require that any of the devices be aware of the other devices. Ethernet is an asynchronous communications method that allows messages to collide and which provides for a collision detection and a random pause and retry means of allowing multiple devices to communicate. Ethernet standards are defined in the IEEE 1802.x series of standards.

3.15
extensible markup language
XML
A meta-language written to allow for the easy interchange of documents on the world wide web or among computers using web based software tools.

3.16
fieldbus
Refers to a digital communication network that connects the field sensors, transmitters and control actuators together and to either a controller or control network. A field bus network allows devices to send and receive messages over a shared path. Devices may send current measurements and/or diagnostic messages and receive commands or configuration data.

3.17
firewall
Refers to a combination of hardware and software installed on computers and network connections to prevent undesired messages from a digital network from reaching or passing through the computers. A firewall may also hide the presence of a computer from other computers on the network.

3.18
field devices
Refers to any sensors, measuring devices, control elements etc. that are used to sense or directly control process conditions.

3.19
front end engineering design
FEED
Refers to engineering activities performed during the identification of project scope and costs. These activities are generally those necessary to develop designs to the point where scope and cost estimates can be supported.

3.20
gateway
Refers to a DCS or other process control system module that interfaces communications between foreign devices or devices within the process control system that use differing communications technologies in a structured and secure manner.

3.21
hazard and operability analysis
HAZOP
A hazard analysis technique for process plant safety analysis in which potential hazards and existing or necessary safeguards are identified.

3.22
heating, ventilating, and air conditioning
HVAC
Refers to systems installed to control the environment in a structure by heating or cooling of air circulated by the system and where necessary, control of air humidity. These systems may also include controls for pressurization of buildings to meet electrical area classifications and limiting of fresh air intake if hazardous conditions exist.

3.23
highway addressable remote transducer
HART
Refers to a communications protocol which provides a means of device communications using a phase shift carrier imposed over a pair of wires. The wires may be dedicated to the communications path or may also carry standard 4 mA to 20 mA analog signals. See www.hartcomm.org for more details.

3.24
human machine interface
HMI
Refers to a computing resource for a process control system that is used as an operator or engineering interface for displaying data or inputting information or operating commands.

3.25
hybrid control system
Refers to a type of DCS that uses open system technologies to perform process control system functions and which is capable of integrating continuous and discrete control functions within a single control module.

3.26
local area network
LAN
A computer network connecting computers and other electronic equipment to create a communication system. These networks commonly use ethernet or similar communications methods.

3.27
Modbus
Refers to an open standard query/response communication protocol that enables communications of numerical and discrete data between automation system devices using a variety of data communications methods. See www.modbus.org for additional information.

3.28
object linking and embedding
OLE
Refers to a Microsoft standard, object linking and embedding, which defines methods for applications to share common data and applications.

3.29
open systems
Refers to technologies that are based upon commercially available, often general purpose, software and hardware that can be obtained from a variety of sources instead of proprietary software or hardware that can be obtained from only one supplier.

3.30opening packaging convention
OPC
Refers to a series of standards, OLE for process control, that define methods for computers to exchange process control related information and application data using extensions of OLE standards. OPC standards provide a common practice for manufacturers of process control systems to make real time data available to other devices in a structured and deterministic way. See www.opcfoundation.org for additional information.

3.31
operability
Refers to the characteristics of a process control system that allow the control system to be operated and maintained in a simple and reliable manner, but still provide all of the functionality and security required of the system.

3.32
personal computer
PC
Refers to a computing resource that has multiple uses. It is intended for use by a single user and may have a number of non-control applications installed.

3.33
process hazard analysis
PHA
A hazard analysis technique for process plants.

3.34
process control module
Refers to some type of computing resource, either of proprietary design or a commercially available computer, which performs process control related functions including data acquisition and control functions.

3.35
process control network
Refers to a digital communications network that is used by process control modules, HMIs or other process control support computers to communicate with one another. This network may use proprietary or industry standard communications methods.

3.36
process control system
Refers to a computer-based implementation of the control and information functions necessary to operate and manage a specific process unit or area. This includes field instrumentation, the communications between field devices and the control processors, HMIs and any other computers and communications required to support or report upon process performance. It does not include general-purpose business computers and networks, desktop workstations or other computing resources not used exclusively to operate, configure or maintain a process unit or area. Safety instrumented systems are not part of the process control system.

3.37
process interlocks
Refer to discrete control functions that cause automatic actions to occur or restrict or suppress automatic actions, but which are not specifically designated as being safety related.

3.38
process safety management
A management process that results in process hazards being identified and suitable safeguards established, and

which provides management of change procedures that ensure that changes to processes are similarly addressed.

3.39
programmable logic controller
PLC
Refers to a control module that performs discrete and some continuous control functions in a module that is generally separate from the DCS or hybrid control system. In refining applications, PLCs have typically performed stand alone discrete or sequence controls. PLCs may also be networked together in some applications or networked to communicate with the main process control system.

3.40
radio frequency interference
RFI
Refers to radio frequency interference that is generated by radios or other electromagnetic communications equipment that may affect the operation of other electronic equipment in an area. RFI may also be generated by the operation of various computing equipment.

3.41
redundant arrays of independent disks
RAID
A distributed storage system spanning disk arrays and automated libraries of hard disks, optical disks, tapes or other bulk storage. RAID applications are often applied to ensure that data is duplicated among disks so that failure of any one disk will not cause loss of function or of the data saved.

3.42
reliability
Refers to the probability that a system or device will perform its function when required.

3.43
remote instrument enclosure
RIE
Refers to an unmanned facility which houses process control systems equipment and other support equipment required for control and monitoring of a process plant or plants. RIEs may be built in place structures, prefabricated structures or simple self contained junction box type enclosures.

3.44
router
A communications network device that learns the location of devices on a multi-segment communications network and reduces traffic on any one segment by repeating messages only for the devices connected to that segment.

3.45
safety instrumented system
SIS
Refers to a system that is intended to protect against specific identified process hazards.

NOTE SIS are not within the scope of this RP.

3.46
safety integrity level
SIL
Refers to the availability required for SIS. SIL is a measure of the probability that the SIS will operate when required to.

3.47
safety module
Refers to a control module that is specifically designed to meet the functional and security requirements for use with

safety instrumented systems. In hybrid control systems, these modules are often integrated with the overall system design.

3.48
safety requirements specification
SRS
Refers to a specification associated with a safety instrumented system that specifies basic functional, implementation, documentation and testing requirements that are to be met in order for the system to satisfy its intended safety integrity level.

3.49
sequencing control
Refers to control functions that involve a series of steps, usually involving discrete controls, that are executed in a pre-defined order and which may be repeated after all steps are completed. Normally, sequencing control is a portion of a larger processing scheme and does not produce a final or intermediate product.

3.50
switch
Refers to a communications network device that controls communications among various branches of the network. A switch electrically segregates network branches and repeats messages to each network branch.

3.51
virtual private network
VPN
The use of encryption to secure connection through an otherwise insecure network, typically the Internet. VPNs are generally cheaper than real private networks using private lines but rely on having the same encryption system at both ends. The encryption may be performed by firewall software or possibly by routers.

3.52
wide area network
WAN
A communications network that uses such devices as telephone lines to span a larger geographic area than can be covered by a LAN.

3.53
workstation
Refers to a computing resource that is used for general business functions such as e-mail, word processing, internet access, etc. but not used as a process control system HMI.

4 Control System Topology

Control system topology is the general layout of the process control system describing interconnections between major components. The system topology should be based primarily on the functionality and security of the control equipment, communications and sub-systems and the technologies being applied. The topology symbolizes the flow of data through the control system components. Management information systems and other non-process control related functions should be segregated from the process control system.

The process control system topology should be developed with consideration of the functions identified as the practices discussed in API 554, Part 1 are applied. The location of each of these functions and associated databases need to be identified to ensure that the proposed design can meet requirements in an economical, secure and safe manner.

These considerations, taken with the design and functionality of proposed hardware and software, will determine the requirements for communication protocols and data transmission methods that will link equipment and sub-systems together.

Figure 2 and Figure 3 show two examples of topology. These are presented as illustrations and other designs exist. Figure 2 represents a typical proprietary distributed control system found in many plants. This system is characterized by a least three communications systems levels with regulatory controls and advanced controls generally being placed at different network levels. Most regulatory control functions are performed using a gateway or directly connected controller with hard wired I/O.

Figure 2 illustrates a modern open architecture system which makes extensive use of digital communications technology to place most control functions on the same network, with modules communicating among one another as required. This design makes greater use of firewalls and shadow databases to maximize system security and isolation from business functions and external networks.

When designing a control system topology and physical location, some of the major considerations that must be addressed are as follows.

4.1 Physical Location of Control Equipment and Sub-systems

The physical location of equipment is important to grouping equipment located in common areas and determining communication needs. The functionality and security of communications may determine what equipment needs to be located in close proximity of one another and which equipment may be located in remote locations. Physical location may necessitate the need for new buildings (i.e. process interface building) or renovations to existing buildings.

4.2 System Availability

System availability considerations will result in redundancy requirements and special topology designs in controllers, highways, communication networks, data acquisition, consoles and field instrumentation. Availability considerations generally also require power distribution systems that provide redundant or backup sources of power. For instance, separate trains of critical equipment are usually controlled from separate subsystems in order to prevent a common failure from taking down multiple trains and these systems are powered in a manner such that single failures will not compromise control or view.

4.3 System Maintainability

System maintainability requirements may include the need to perform diagnostics and system maintenance functions such as software updates from remote locations. This will dictate topology requirements for data links and communications in order to facilitate this process. Additional control module redundancy may be necessary to meet system maintainability.

The characteristics of the process being controlled must also be considered when considering the maintainability of the process control equipment. Provisions should be made for major maintenance or upgrades that can only be performed when the process is shut down. In large complexes, this means that equipment should be segregated so that processes areas that cannot or do not come down together do not share key equipment.

4.4 Control System Performance Requirements

Special control performance requirements such as rapid response times for operating valves or updating displays may require dedicated controls, separate communications networks or local controls that will be reflected in the topology of the system.

4.5 Lifecycle Costs

Both installed costs as well as all lifecycle costs need to be considered in designing the topology of the network. When the need for redundancy or robustness of equipment and systems is considered, potential costs of system

failure in terms of personnel safety, equipment integrity and production costs must be considered and often provide justification for more robust and secure designs.

4.6 Security of Control System

Security considerations that affect the topology of the control system include firewalls, DMZs, communications servers and restricted data links. Most of these issues must be identified and addressed during the process control system functional specification development process described in API 554, Part 1. Also, See ISA 99 for extensive discussions of process control system security issues and resources. A detailed discussion of process control systems security is a complex and arcane issue and is beyond the scope of this document, although some basic considerations are described in 7.1.

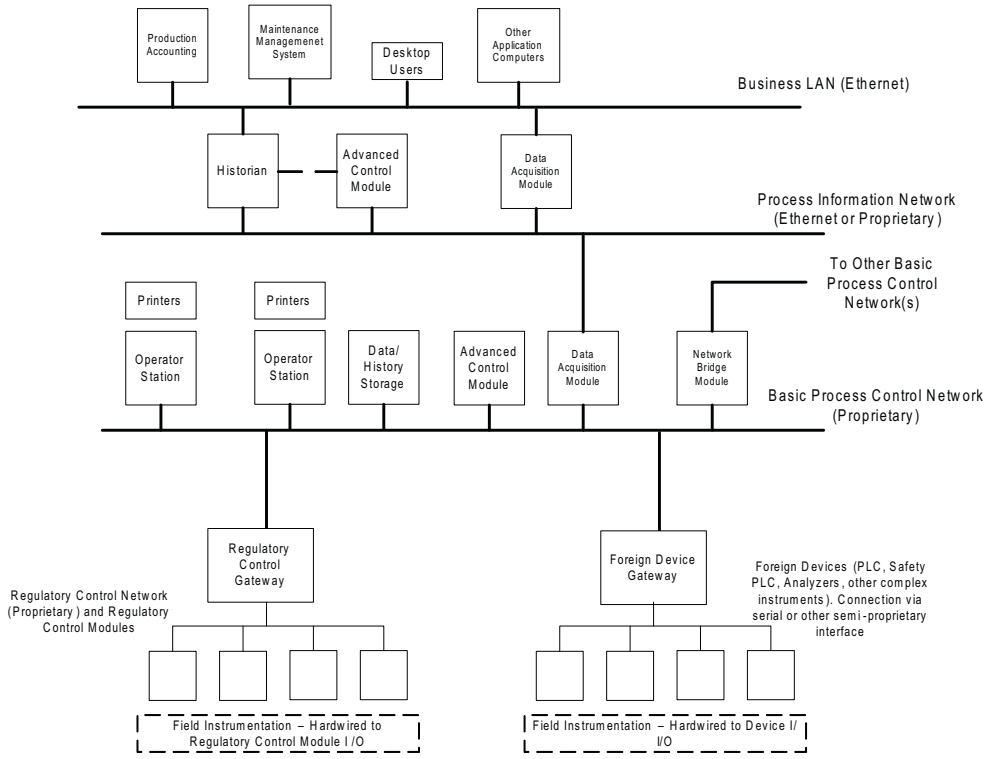

Figure 2—Control System Topology

5 Process Control System Types

There are several types of systems that may be used a part of a process control system. The selection of hardware and software implemented in a specific process control system should be based upon the functions identified during the processes described in API 554, Part 1. As part of the specification and selection process, the user and engineer must define the functions that will be implemented and what types of architecture, communications and hardware will be used.

Historically process control systems were implemented using a combination of a proprietary DCS system that handled most continuous control functions and potentially several specialty sub-systems, often provided by third parties, which would handle functions that the DCS was not able to perform. Examples of these sub-systems are PLCs, safety logic solvers, analyzers and equipment monitoring systems. Usually these sub-systems require additional hardware and software to interface them with the DCS.

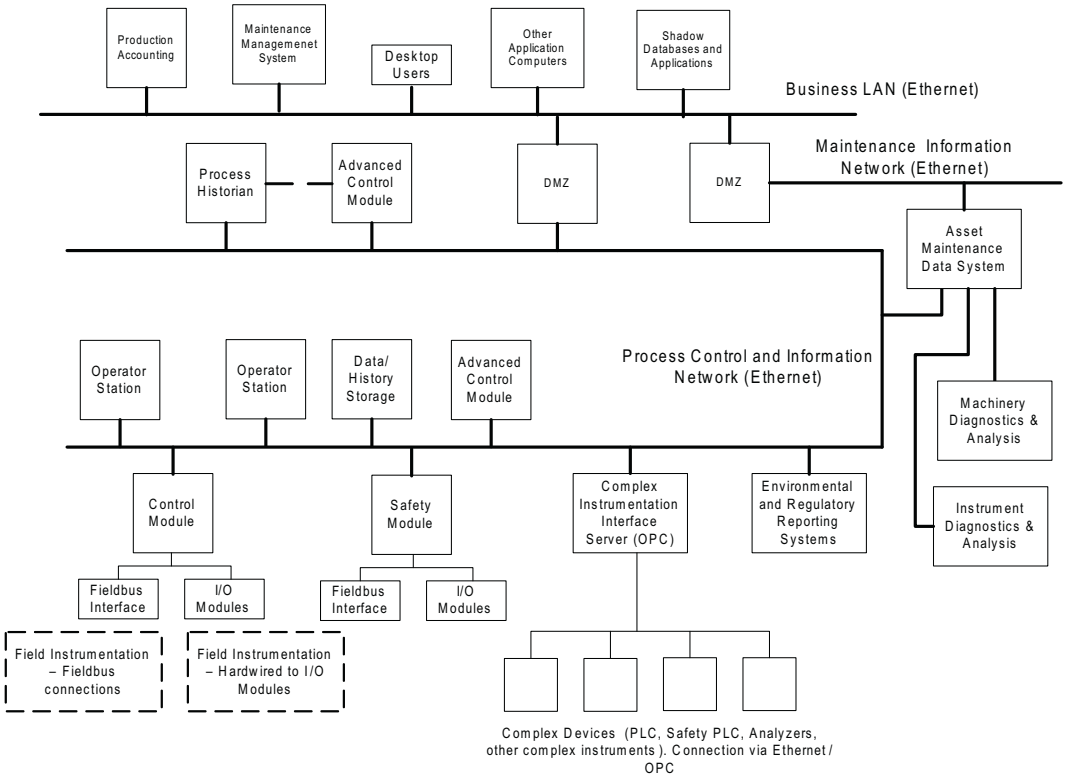

Figure 3—Control System Topology—Open Architecture Hybrid Control System

The proprietary DCS system has evolved into hybrid process control systems that are capable of performing many more functions than the older systems could readily perform. This includes integration of many discontinuous functions.

5.1 Distributed Control Systems

A proprietary DCS is a microprocessor-based control and data acquisition system, comprising multiple modules operating over a network. The hardware and programming of all devices in the system are developed by the manufacturer using proprietary designs and generally cannot be interconnected with other equipment without use of customized gateways.

The system functions can be geographically and functionally distributed. Hardware consists of the general equipment listed below.

— Control modules that provide data acquisition and various control functions. These modules consist of physical enclosures, input/output modules, processors and other power and communications support for the module to function. The control strategies are programmable and there are many standard, special and optional functions available. Normally, the programming and configuration of the systems uses manufacturer specific algorithms and procedures. These controllers are primarily used for continuous or batch processes. Several controllers can share data through a common network. These controllers can also be redundant for critical applications. Depending upon the system design, there may be additional modules that perform data acquisition functions with no control functions.

— Operator shared display interfaces that display process values, statuses, alarms and other functions. These have historically been propriety hardware and software designs, though more open system retrofits have been

available using standard PC equipment, but with proprietary software to drive the displays to mimic legacy functions.

— Communications networks to provide robust communications among DCS equipment. This is typically a proprietary closed design provided by the DCS manufacturer.

— Specialty modules to provide historization, advanced control and data storage functions.

— Gateway modules to provide a variety of interfaces to third party sub-systems or computer systems. These are usually proprietary design modules that interface to open systems communications such as ethernet, Modbus or other technologies.

5.2 Programmable Logic Controllers

Programmable logic controllers are microprocessor-based solid-state devices which are programmed to operate in a particular sequence in response to external inputs. PLCs can be used in place of relay systems or for proportional, integral, and derivative (PID) control in specific applications. A typical PLC consists of a programming unit, a processing unit, an I/O unit, and a power supply.

The control strategies are programmable and there are many standard, special and optional functions available. These controllers are primarily used for discontinuous applications, but may also include continuous control functions. Current technology PLCs provide more powerful and user friendly continuous control functions than many earlier versions and in some applications can act very similar to control modules. However, they also contain many machine control oriented functions that are not typically used in process applications.

Several controllers can share data through a common network. Some controllers can also be redundant for critical applications, and be directly interfaced to a hybrid control system only if the PLC manufacturer has worked with the hybrid control system vendor and provides certified hardware and software interfaces. A much more typical implementation is through interface servers that use standard methods, such as OPC.

PLCs may be applied in several roles and are often used in specialty applications provided by third parties. The process control system functional requirements should be considered when applying PLCs. While designs vary, PLC applications are typically less robust than integrated process control systems (DCS or hybrid systems) and are often more complex to implement in larger systems.

Some of the applications for PLCs are as follows.

— A stand-alone PLC that is capable of performing control functions associated with a number of smaller applications within a process area, or one large function such as sequence control, particularly when a third party is supplying a package sub-system.

— An integrated PLC that is designed as an integral part of a general purpose process control system that performs all of the functions required of the process control systems.

— A small single purpose PLC that has limited functions and input/output capacity. These are often used as independent controllers for a more sophisticated instrument or mechanical device.

The programming techniques commonly used to express sequential on-off logic include ladder diagrams or Boolean logic, although many models are also available with IEC 61131-3 compliant function block programming. Programmable controller logic resides in a memory, which can be modified to allow for changes in the applications or to correct errors in the initial programming, usually without shutting down or interrupting the process, provided that these changes are carefully made with adequate management of change and planning.

5.3 Single Loop Controllers

There are three basic types of single-loop controllers. Selection of these controllers is determined by the degree of integration with other systems.

Digital electronic. The input/output signals are usually 4 mA to 20 mA DC, but may also be a fieldbus or other digital communications. Digital controllers contain a microprocessor and the control functions are programmable. They have a variety of standard functions that can be used for control applications both continuous and discrete. Some digital controllers have the capability of networking with larger distributed control systems.

Analog electronic. The input/output signals are usually 4 mA to 20 mA DC. Circuitry in the controller is based on analog electronic techniques.

Pneumatic. The input/output signals are usually 3 psig to 15 psig (20 kPa to 100 kPa) and can be direct connected to the process. These instruments provide local control capability using mechanical technology that uses process fluids and/or compressed air.

5.4 Hybrid Process Control Systems

Current technology process control systems are often referred to as hybrid process control systems. This terminology originates from the fact that the functions performed by the systems combines functions that previously required separate sub-systems for continuous control and discontinuous controls (e.g. a proprietary DCS with external PLCs or a PLC based process control system). The hybrid process control systems also are often capable of performing many advanced control system functions such as multivariable control, batch control, etc. without requiring external process control computers.

Hybrid process control systems have the following general characteristics.

— Control module functions are based upon industry standard functions, typically, IEC 61131-3. These functions provide for performing both continuous and discontinuous control functions and provide for ready integration of these functions. Control module designs are usually still proprietary and use proprietary software.

— Operator interfaces are based upon standard PC technologies instead of proprietary hardware. The software that drives the displays is usually proprietary, though some general application interface software is available.

— Communications technologies are industry standard, usually ethernet. The network technologies also can support a variety of communications media (copper wire, fiber optic and wireless) using industry standard interface equipment such as internet switches, routers and bridges.

— Interfaces to third party equipment is performed on industry standard hardware (usually a PC) and uses industry standard interfaces such as OPC, Modbus, etc.

5.5 Transitional System Designs

Many proprietary DCS suppliers have provided some degree of upgrade capability as they have changed their system offerings from the proprietary DCS to hybrid process control systems. Typically, these offerings have the following characteristics.

— Replacement of proprietary DCS operator interfaces with the hybrid process control system operator interfaces.

— Overlay of the proprietary DCS communications networks with gateways to the hybrid process control system communications networks. This functionality typically allows the existing proprietary DCS control modules to

continue to operate with operator interfaces and other higher level functions being implemented on the hybrid process control system.

— Retrofit packages that allow hybrid process control system control modules to be retrofit to I/O terminals and wiring of existing proprietary DCS control modules.

5.6 Safety Systems

Safety systems are designed to operate independently of the process control systems and have specific required practices relative to data communications and management of software and programming. Many hybrid control systems offer safety modules that integrate with the rest of the process control system, but still meet the communications and management requirements appropriate to safety instrumented systems.

Many stand-alone safety systems also exist that are programmed independently of the process control system, but which have communications functions that send data to the process control system.

6 Process Control System Hardware Design Considerations

6.1 General Considerations

The process control system architecture will consist of many different devices, potentially installed in a number of different locations. Typical examples of process control system architectures are shown in Figure 2 and Figure 3. This section discusses many of the considerations that need to be addressed in selection of various hardware and software components of these systems. Among the issues that are discussed are:

— overall system design, equipment location, routing and redundancy;

— selection of control modules;

— selection and application of field communication networks;

— selection of operator and engineering workstations;

— selection of I/O modules;

— software selection;

— expansion capacity; and

— maintainability.

6.2 Overall System Design

Prior to detailed specification of process control system components, the overall system design must be determined. API 554, Part 1 describes many of the considerations that go into this process, and generally the process control system functional specification described in API 554, Part 1 will provide the basis for making final definitions. These design criteria should address the following.

— The general physical layout of the process control system including the location and approximate layout and size of control centers and satellite control houses, field enclosures and other equipment.

— Power supply system and distribution requirements including AC and DC power supply redundancy requirements.

— Lightning protection and grounding requirements for both electrical safety and the process control system.

— The approximate equipment requirements, including the number and sizes of operator HMIs, requirements and locations for engineering stations.

— The number and sizes of control equipment cabinets or other enclosures, including the approximate numbers of control modules and I/O modules and associated accessory equipment.

— The number and location of higher level computers or other control computing resources and the number and location of computers or computing resources required to support other business functions.

— Requirements for hard-wired connections from the process control console to the units or remote instrument buildings. This includes items such as connections to hard wired shutdown switches, dedicated alarms or other dedicated functions.

— The location and installation of development or test hardware and software to support software upgrade testing and development of new or modified control applications.

— The types, general layout and routing of field buses and other communications connections with field instrumentation and systems.

— The types, general layout and routing of process control and business communications networks. This includes peer-to-peer process control communications, hierarchical communications, field networks and business networks.

— Provision for control of hardware and software maintenance/upgrades, configuration changes, process equipment changes, operator certification and re-certification, emergency preparedness, and vendor support of the process control equipment and the process equipment.

— Safety system requirements such as integrated or independent hardware and software and the required communications.

— Interfaces with other complex systems such as analyzers, machinery monitoring or other similar applications.

— Operating and maintenance communications systems requirements such as radio, telephone and video.

6.3 Controllers

The controller for the process control system gathers information from the I/O modules and other devices in the system. The processors within the controller perform the required functions needed to provide information to the final control devices or other systems/devices. These functions are configured into the controller by the system integrator, design engineers or owners control staff. See API 554, Part 3 for information regarding staffing and responsibilities.

Typically, controllers should be able to execute commands using the following functions and parameters. See API 554, Part 1 for a list of general functions:

— PID and process control functions;

— alarming functions; analog, discrete and system;

— batch and sequencing control;

— logic and math functions;

— time delays, counters, and timers.

Some additional design considerations for controller include the following (see 6.11 for a discussion of redundancy and redundancy performance):

— the controller should retain its memory in the event of power loss;

— the controller should be modular and removable for maintenance;

— the controller real-time clock should be synchronized to a common system clock and have resolution capable of supporting required time tagging of events;

— the controller should be capable of scanning and updating the I/O, executing logic and analog functions, and supporting communication interfaces to achieve required performance (typically, logic functions—ten times per second and analog functions—four times per second);

— when combining discrete and analog functions in one controller, the analog functions increase the execution time and should be taken into consideration.

6.4 Operator Interface

Operator stations provide the primary means of operating the process and conveying the operator's commands to the process control system. Typically, an operator station is located in a control room. An operator station consists of a display screen/s, keyboard, mouse, etc. that allows the operator to interact with the process control system. Typically, an operator's console consists or multiple independent operator stations.

There also may be specialized functions that are integrated with the operator's console. These include emergency shutdown switches, critical systems annunciators, and special purpose interfaces such as vibration, fire and gas or other independent systems.

Design considerations for operator interfaces are as follows.

— The update times for display screens should be as fast as possible to provide a real time view of the process. Due to system limitations the update time is typically 1 to 4 seconds.

— Screen layouts need to be based upon the capabilities of the actual device and follow consistent, approved corporate standards, such as equipment placement, direction of flow, line thickness and color, number of real-time values per display, etc.

— The number of operator stations will be determined by the size and complexity of the process being controlled and the number of operators assigned to the unit or process complex.

— Ergonomic considerations should be taken into account in the design and layout of the operator interfaces. Items to consider should include the room arrangement, lighting, climate, air purity, and sound levels. See Section 11 for control center design considerations.

— Wireless operator interfaces are becoming available, but are not yet in widespread use. Reliability and security of these devices is still developing, so functionality tends to be limited to indication or information use.

6.5 Engineering Workstation

Separate engineering workstations may be required to configure the subsystems of the process control system (i.e. DCS, PLCs, SIS, analyzers, vibration monitors, etc.). When engineering workstations are used then the workstation

would consist of electronics, storage media, display screen, keyboard, and printer to allow authorized personnel to configure, download, monitor, trend, document, modify, and verify software configuration.

6.6 I/O Modules

Input/output modules are the interface between the field instrumentation and the process controller. These modules may be integral with the process control module (e.g. communications, control processors mounted on the same back plane as the I/O modules) or may be remotely mounted.

Common considerations for selection of I/O modules are as follows.

— Signal types and levels that will be handled by the modules. Typical I/O modules are analog input, discrete input, discrete output, analog output, frequency, thermocouple, RTD or digital communications. The I/O modules typically are packaged in racks and the modules are usually multi-channel (i.e. 4, 8, 16 or 32 channels).

— In many systems, I/O modules are available for communications with various digital systems such as Fieldbus, HART or other serial data communications.

— Power sources and isolation for the I/O module channels.

— Wiring methods to be used and space required for the modules.

— Installation environment—are the modules installed with the controller and communications modules or are they remote? What are the ambient conditions and/or electrical classification requirements? Is cooling, heating or purging required for safe and reliable operation? What potential effects of EMI or RFI exist and how must they be mitigated?

6.6.1 I/O Module General Design Issues

The format, location and environmental installation requirements for all I/O modules must be considering in selection of the line of modules to be provided and how they will be installed.

— The location and environment of the installation must be considered in selecting the modules. If the modules are to be located in remote locations, they may need to be capable of withstanding ambient temperatures and area classification. Purging of I/O enclosures may be required for electrical or area cleanliness purposes.

— The power supplies to the I/O modules and the I/O channels must be identified and appropriately designed. Power for the modules themselves will likely have to be supplied for the same source, or one of equal reliability, as the process control modules. The power requirements for I/O channels must be defined. Many modules require external power, or have limited capabilities to provide I/O power. Power supplies must be suitable for the area classification and ambient temperatures in which they will be installed.

— If the I/O is remote from the control modules, the communications to the remote I/O must be evaluated for suitability. The impact of loss of communications must be assessed and the need for redundant and/or separately routed communications must be identified.

— I/O module performance upon wiring faults, missing wiring or unused channels needs to be assessed to ensure that faults are properly alarmed, and that unused channels do not cause nuisance alarms.

— I/O must be electrically protected from field device and wiring faults. Typically, current limiting resistors or fuses are provided internally or externally. Modules that are used in intrinsic safety designs may require special models

or external barriers. Installations must be protected from induced or stray voltages that may generate false signals.

— I/O module redundancy should be carefully evaluated to ensure that failures do not unacceptably interrupt ongoing operations. Many I/O module designs allow for redundant I/O processors that share a common passive wiring panel. The mechanisms by which spare I/O modules are switched in should be evaluated. For example some process control systems allow spare modules to be switched in independent of other modules while others use a rack-to-rack failure swap in which an entire set of I/O modules are swapped upon failure in any one module.

— All I/O modules should be remotely configurable and publish their entire configuration on request.

— The I/O system design should allow for removal of any failed module, whether redundant or non redundant, without affecting the operation of any other modules.

6.6.2 Analog Input Modules

Analog input modules convert analog signals from transmitters into a digital signal that can be used in the process control system. Different style input modules may be required for 2-wire and 4-wire transmitters depending on the manufacturer of the module to address power supply and isolation issues. Typically, input modules can be configured to do filtering, characterization and other functions. Fusing or internal current limiting should be considered internal or external to the module in order to prevent damage. Typically, designs which are inherently current limiting should this signal be shorted are preferred to designs that require fuses.

Analog input modules should also be capable of accepting signals from externally powered devices or other devices in which the local ground may be different than the I/O module ground. If this functionality does not exist, additional isolating modules may be required.

6.6.3 Analog Output Modules

Analog output modules convert digital signals from the process control system that can be used by the final control element or other system/device. Typically, output modules can be configured to do filtering, characterization or other functions. Fusing or current limiting should be considered internal or external to the module in order to prevent damage.

Analog output channels have limitations on the load that can driven. This can be a factor in designs that require several final control elements to be driven by the same output, such as split range control valves. Also smart valve positioners provide a higher load than passive devices, and this may limit the number of devices that be connected to an output.

6.6.4 Discrete Input Modules

Discrete input modules convert status contacts into digital signals that can be used in the process control system. They can accept a variety of voltages and care must be taken to insure that the signals are compatible with the module. Often, discrete input modules provide sensing voltage (typically 24, VDC) at low current supply. Interposing relays may be required due to load and safety considerations. Typically discrete input modules have LED to indicate the status of each input, low-pass filters to reduce the effects of noise and bounce, and opto-isolation to protect the module. Fusing or internal current limiting should be considered internal or external to the module in order to prevent damage.

6.6.5 Discrete Output Modules

Discrete output modules convert digital signals from the process control system that are sent to the final control element or other system/device. The output can be solid-state or relay contact. The user should evaluate failure

mechanisms and reliability before selecting the type of output. For example, some solid state designs have indeterminate failure mechanisms, while relay outputs usually have more clear failure mechanisms.

The modules must be specified to meet the voltage and current requirements of the connected load. Interposing relays may be required due to load and safety considerations. Typically discrete output modules have light-emitting diodes (LED) to indicate the status of each output, and opto-isolation to protect the module. Fusing should be considered internal or external to the module in order to prevent damage.

It is important to determine where the power source for the load will be and at what voltage and current levels. Some modules can supply power to the load and others require external power. Installations should be reviewed to ensure that outputs of differing voltages and AC and DC loads are properly isolated from one another, and that excessive current loads, voltages or other electrical limits of the I/O modules or cabinet design are not exceeded. For example, a single high voltage signal may trigger a code requirement to raise the wiring insulation specification for the entire cabinet.

6.6.6 Thermocouple Input Modules

Thermocouple input modules convert signals from thermocouples into a digital signal that can be used by the process control system. The type and linearization of the thermocouple is configured in the control system. Some manufacturers have specific modules for each type of thermocouple.

6.6.7 RTD Input Modules

RTD input modules convert signals from RTDs into a digital signal that can be used by the process control system. The type and characterization of the RTD is configured in the control system. Some manufacturers have specific modules for each type of RTD.

6.6.8 Other Types of I/O Modules

There may be other types of I/O modules required to bring special signals into the process control system. These would include pulse, frequency, vibration, digital communications or fieldbus signals.

6.7 Serial Digital Communications

Most complex instrumentation, such as analyzers, machinery monitoring systems, stand alone controllers, and similar instruments, provide methods for the instrumentation to communicate a large amount of process, status and internal configuration data to the process control system. In some applications, there may be a need to have many such devices communicate with the process control system. Some of the criteria that need to understood in order to define a design are described as follows.

6.7.1 Communications Protocol

The instrument manufacturers will state what protocols their devices support and what physical connections are available. Most manufacturers support Modbus or HART protocols, and some will support an OPC interface. During definition of the process control system design, the numbers of devices that must be interfaced with the process control system must be defined.

The capabilities of the process control system must also be reviewed to verify that the system is capable of handling the communications, and to determine how many independent communications channels may be needed. The process control system design must also be reviewed to identify the method by which values being obtained are configured and presented to the operator and historian.

6.7.2 Physical Communications Layer

The physical communications layer that is selected will depend upon the instrument manufacturers capabilities and the requirements of the process control system. Some of the common physical communications used are as follows.

— *RS-232*. This is a single device serial communications layer that can be used over short distances, typically no more than 50 ft. When longer transmission distances are required, another physical layer must be used, or a protocol converter is used.

— *RS-422*. This is a single device serial communications layer that can be used over longer distances dependents upon data rate and communications media specifications.

— *RS-485*. This is a single or multi device serial communications layer than can be used over longer distances. It is possible to implement a multi-drop RS-485 network by daisy-chaining a number of RS-485 devices, however, this must be carefully done. Many times, devices from different manufacturers whose specifications claim RS-485 compatibility will only be compatible with other devices from the same manufacturer.

— *Ethernet*. A greater number of devices are being provided with the capabilities to communicate using an ethernet physical layer. This provides a means of connecting an number of devices to a single network, but compatibility and use of consistent data protocols must be confirmed. A common data protocol when ethernet is used is Modbus over TCP/IP.

— *HART*. HART protocol is used over a two wire connection to an instrument and may be multi-dropped in some implementations.

— *Other proprietary systems*. Some manufacturers may support their or other manufacturer's proprietary communications. For example, some manufacturers many support use of some PLC manufacturers communications networks.

6.7.3 Process Control System Interface

The interfaces to serial communications available vary by process control system manufacturer and the type of hardware being provided. Some of the more common configurations are as follows.

— An input/output module that is designed to be installed in a control module and which can support a limited number, usually one or two, of serial communications networks, and which allows values or status indications to be addressed using a limited selection of protocols. For example, a serial I/O card may support two networks using RS-485 communications and Modbus data protocols. Some HART serial interface I/O modules can accommodate up to eight or more HART networks.

— A gateway that is connected directly to the process control network that provides much the same functionality as a serial input/output module.

— A gateway that supports general purpose serial communications, usually using ethernet communications and OPC data exchange.

6.7.4 Single Drop vs. Multi Drop

A serial network's physical communications design and protocol may allow several devices to be attached to one network. Selection of a design that has multiple drop capability must consider a number of issues.

All devices must be compatible with the communications and with each other. This is often difficult to assess as specifications for various devices may state compliance with a specific standard, but in practice, they only work well

with other devices from the same manufacturer, and often from the same model line. Many, many hours can be consumed attempting to find the combination of settings that results in multiple devices communicating reliably.

When working with multiple devices on a serial network, a practical practice is to provide protocol converters from the same manufacturer at each device. A wide range of converters are available including RS-232 long haul modems, RS-232/RS-485, RS-422/RS-485 and RS-485/RS-485 isolating converters. This design has the benefit of the polling gateway seeing devices from the same manufacturer and any setting issues associated with the source device can be handled within the protocol converter configuration.

6.7.5 Process Control System Data

The data format and capabilities for data read from serial communications will vary with the process control system manufacturer and implementation. These must be reviewed against functional requirements in order to ensure that the installation meets the functional requirements for the installation. Some of the issues are as follows.

— Most serial interface equipment provided by a process control system is non-redundant and decisions upon what signals to place on a serial input network, and how many networks are required must consider the fact that a fault on the network or its interface equipment may result in loss of view of the data.

— The selection of data that will be transmitted over a serial network also must consider the latency of the communications. Once characteristic of these communications is that they often are relatively slow, with update times typically being 5 seconds or more.

— The implementation of serial data values may have limited functionality relative to conventional I/O values. Some examples of this are that values may have no or limited alarm capabilities and in some implementations, the data appears as a value in an array or list that has no designation of the value's service or tag number. Additional programming may be necessary to provide even the most basic tag functions.

6.7.6 Network Testing

Because of the numerous settings that require adjustment during commissioning of a serial network, it is recommended that as much testing as possible be done prior to commissioning. Wherever possible, bench testing of all devices together with the process control system interface should be performed and the settings required to make the entire system operate recorded for field set up.

If network testing cannot be performed until the field installation is complete, adequate time for set-up testing and troubleshooting must be allowed. Testing and debugging a complex serial network consisting of multiple devices can take several weeks of intensive effort.

6.8 Field Networks

Most new process control systems can make use of one of the several available fieldbus technologies. The technology used should be selected according to the process control system functional requirements. Some technologies such as Foundation Fieldbus have been functionality directed towards continuous control and measurement. Others such as Profibus perform well when discrete devices are used. Still others such as Devicenet are more applicable when significant numbers of simple devices are used in a limited area (such as use for machine control). Table 2 illustrates the characteristics of different types of fieldbuses. See IEC 161158 and the ISA publication *Fieldbuses for Process Control*.

In addition to the general performance properties identified above, each fieldbus technology has its own limitations and requirements relative to power supplies, network length, wiring requirements, redundancy, number of devices that can be connected to any one segment and intrinsic safety requirements.

Table 2—Fieldbus—Device Network Classification

	Sensor Bus	Device Bus	Fieldbus
Message Size	< 1 byte	Up to 256 bytes	Up to 256 bytes
Distance	Short	Short	Long
Data Transfer Rate	Fast	Medium to fast	Medium to fast
Signal Replaced	Discrete	Discrete or analog	Discrete or analog
Device Cost	Low	Low to medium	Medium to high
Component Cost	Very Low	Low	Medium
Intrinsic Safety	No	No	Yes
Functionality	Low	Medium	High
Device Power	Low	Medium	High
Optimization	No	No	Yes
Diagnostic	No	Minimal	Comprehensive

6.9 Complex Instrumentation

During process control system design, the planned use of complex instrumentation that may be used, and the means by which it will communicate with the process control system must be considered. For example, many analyzer systems, machinery monitoring systems or specialized machinery control systems are capable of directly communicating with the process control and Information network or with a maintenance data network (see Figure 3). The type of communications and variables that will be read or written must be identified.

6.10 Sub-system Interfaces

The process control system may have different specialized subsystems that need to communicate to other subsystems through general-purpose digital communication interfaces. Ideally this would provide high-speed information exchange between subsystems. These interfaces should be standard protocols with standard port configurations such as those described in 6.7.

6.11 Redundancy

Redundancy is the use of duplicate components to increase the reliability and availability of the process control system. The extent of redundancy should be determined early in the project based on the criticality of the process and economics of the project. Typically, redundancy would be considered for communication networks, controllers, power supplies, operator stations and I/O modules

6.11.1 Communication Networks

There are several communication networks involved with a process control system. Normally the network between the controllers and operator consoles and the network between the controllers and the I/O modules would be redundant. Other networks that connect to third party devices should be considered on an individual basis. A redundant communication network would be designed such that no single point of failure would cause any device on the network to be unable to communicate to the rest of the network. The physical installation of the network cabling should be considered and appropriate separation should be provided.

6.11.2 Controllers

Redundant controllers are designed to be fault tolerant so that one of the controllers is always operating. When the active controller fails, the other controller will automatically take control. An alarm will be displayed on the operator console to indicate that a controller has failed. The failed controller can be replaced on-line (dependent on the

manufacturer procedures). The new controller should be configured automatically by the control system when it is installed, although some systems require a manual download of data.

6.11.3 Operator Stations

Operator stations should be fully independent and operate in a manner that view of the process would not be lost if one or more stations were to fail.

6.11.4 Input/Output Modules

Most process control systems offer a variety of redundant or non-redundant I/O modules. Normally, these modules will share a passive wiring terminal assembly.

The selection of redundant or not redundant modules should be based upon assessment of operability and safety. This assessment must consider potential unplanned capacity loss or reduced operability and safety should an I/O module fail. In some installations, controller I/O may be redundant while indication or process alarm functions may not have redundant I/O.

Certain safety instrumented systems require redundant I/O modules. An alarm will be displayed on the operator console to indicate that an I/O module has failed. The failed module can be replaced on-line (dependent on the manufacturer procedures). Certain modules require configuration that should automatically be configured by the control system when installed.

6.11.5 Power Sources

See Section 11 for a discussion of power distribution.

6.12 System Capacity/Future Expandability

The system capacity for each subsystem of the process control system should be adequate and allow for future expansion. This must include controllers, input/output modules, rack space and power supplies.

6.12.1 Controllers

Controllers should have adequate memory and software to handle the system performance requirements and allow for additional control points to be added. Typically, this is a minimum of 10% to 20% spare capacity. Additional capacity if the process has the potential for significant automation upgrades.

6.12.2 Input/Output Modules

Each sub-system should be designed for a minimum capacity of the point count at the time plus 30% when purchased to allow for additional points that will be identified during the further project development. This should allow for at least 10% installed spare capacity at the time of installation, plus physical space and system support capacity for at least another 20% I/O modules and support equipment.

6.12.3 Rack Space

The necessary space requirements for racks, or bases have been anticipated such that expansion of I/O points in each process input/output device is by the addition of only I/O modules and interconnecting cables.

6.12.4 I/O Expansion

Expansion of I/O points or geographical coverage should be possible with the addition of process input/output devices without a shutdown of the communication network or process control device.

6.12.5 Power Supplies

Power supplies should be sized or be modularly expandable to accommodate all anticipated expansion. See Section 11 for a discussion of power distribution systems.

6.13 System Performance

The system hardware and software should have execution times that meet or exceed the time constants of the process being controlled. Performance requirements should be met under conditions of peak loading and include loads for all data functions such as data collection, reporting, alarming, etc. Some functions that require extremely fast scan times, such as compressor surge control, may require a special control system. The system software should be configured to meet the performance requirements of the process. Putting fast scan times on all functions will affect the capability of the system to perform properly. Scan times should be optimized so that the system is not overloaded, or capacity wasted.

Many proprietary DCS systems had very deterministic designs—in effect, capacity was fixed and difficult to modify. Newer hybrid control systems have control modules that are not deterministic: the number of functions and execution speed interact and a user can chose to program a controller to be lightly loaded and run at fast cycle times, or be heavily loaded and run at much slower cycle types. The user must be cognizant of the these trade-offs and ensure that the control modules are suitably programmed.

6.14 Diagnostics

The process control system should incorporate comprehensive self-diagnostics so that all permanent and transient faults are identified, located, alarmed and reported. All diagnostics should be performed automatically on-line, without disturbing the process or reducing the reliability of the system. On-line diagnostics should perform the following functions:

— test all boards in the system;

— perform power-up diagnostics on the control system;

— perform diagnostics on all processors;

— perform diagnostics on all I/O boards;

— perform diagnostics on random access memory (RAM) and read only memory (ROM);

— perform diagnostics on system communication highways;

— monitor environmental conditions, such as cabinet or module temperatures to alert of conditions that could lead to degradation or failure;

— verify that redundant processors and programs are good and current; and

— provide status and fault information using board level LEDs, displays, alarms, etc.

6.15 Maintainability

The control system hardware should be located where it can be repaired and maintained. Consider weather protection for hardware located outdoors.

All modules should be replaceable with the system powered. Modules should have mechanical keying to prevent physical insertion and on-line activation of a module in an incorrect slot in the chassis. Shorting or grounding the field wires connected to any I/O module shall not damage the module itself.

7 Process Control System Software Design Considerations

7.1 Operating System Considerations

A major consideration in implementation of a process control system is a full understanding of the operating system and the support requirements imposed upon the user of the system. Almost all process control systems have moved from use of closed systems based upon proprietary and limited implementations defined by the process control system supplier to use of widely available commercial operating systems. The preponderance of these systems are based upon Microsoft Windows operating system plant forms, although other platforms such as UNIX or VMS are available from some suppliers.

Use of general purpose commercial operating systems has resulted in a number of unintended but substantial consequences. Some of these are discussed below. This is not an all-inclusive list of issues, but is intended to highlight the types of things that must be recognized and included in the support plan. See ISA 99.00 for additional discussion of security issues.

7.1.1 Functional Lock Down

Commercial operating systems offer an extensive range of functions, most of which are not necessary, nor are they desirable, in process control system applications. The user must understand these functions and ensure that they are not accessible in the installation of the process control system. The process control system supplier should take responsibility for ensure that the implementation as sold meets the customer expectations and provide a system suitable for the applications. Some of the issues are:

— access to functions that allow addition of software or use of non-process control functions such as e-mail, word processing, spreadsheets and games is prevented;

— access to general purpose storage devices such as USB-based mass storage devices is disabled except when necessary for system maintenance; and

— only those communications ports absolutely necessary for system operation be open, and even these be tightly regulated.

7.1.2 Patches and Upgrades

Commercial operating systems usually have routine patches and upgrades issued by the operating system supplier. Some of these may be necessary to support continued process control system operation, but many are not. Operating system patches should not be directly applied to operating process control systems. The process control system supplier should have a process by which recently issued patches are tested by the supplier to verify that they have no impact upon their software and then should be rolled out to the users of these systems. This must take place in a timely manner to prevent users from being exposed to operating system security problems for extended periods of time. Use of a small test or training system to validate software upgrades and patches prior to installation on an on-process system should be considered.

7.1.3 Virus Scans

Commercial virus scan programs should not be applied to process control system software unless the process control system supplier expressly recommends it. Running of virus software of process control system modules can negatively impact operation by delaying delivery of information to the operator or other process control system functions.

Virus prevention is a critical aspect of operating a process control system, but must be implemented in a manner that does not have the potential to impact continuous operations. Prevention of virus propagation must be an integral part of the process control system design by limiting of communications with outside systems and preventing hand-carried propagation by disabling external storage devices such as plug in memory sticks, USB storage, etc.

7.1.4 Hardware Interoperability

Commercial operating systems support a wide range of readily available and interchangeable components. However, the supplier of a process control system usually has based software operation and certification upon a limited number of components such as processors, memory, graphics adapters, mass storage, etc. Off-the-shelf components should not be used prior to certification by the process control system manufacturer.

7.2 System Programming

There are two distinct processes to software design; configuration and programming, though the more modern IEC 61131-3 based process control systems have blurred the distinctions. The software should be designed to meet the requirements of the process being controlled. It takes planning between engineering, operations and control engineers to configure and program the control system.

7.2.1 Configuration

Configuration sets the basic control system parameters for such functions as:

— hardware addressing;

— I/O card/module types and quantities;

— I/O parameters and engineering units;

— standard alarming functions;

— standard history and trending;

— standard operator displays;

— standard process control algorithms; and

— communications protocols.

7.2.2 Programming

Programs are developed for the control systems:

— complex or advanced process control;

— batch control;

— event-based control;

— interlocks;

— reports and logs;

— safety shutdown programs;

— sequencing;

— special alarming; and

— transferring data to/from external networks.

7.3 Configuration and Programming Devices

Various types of programming devices are available depending on the control system. Typically, the configuration/ programming software runs on a personal computer which may or may not be integrated with the process control system.

This personal computer is used for program development, simulation, graphics development, forcing, storage, fault diagnostics, system monitoring, and application documentation. The configuration/programming may be developed in “offline” mode on a stand alone personal computer or in “online” mode on a PCconnected to the control system either directly or through a network (see 6.5).

7.4 Configuration/Programming Considerations

Process control system configuration and programming consists of several activities.

7.4.1 System Setup Configuration

System setup configuration consists of all activities necessary to define to the process control system what modules and functions exist, their network or system addresses and names, I/O modules available and to define basic system rules (e.g. who can write to what, what data is saved, etc.). This activity also includes setting up of user IDs and definitions of what rights each user has to view, operate or modify the system, and to which process areas these rights apply.

7.4.2 Basic Process Control System Applications

This activity involves all activities required to define input/output tags and associated I/O addresses, and to define all application data for the tags such as ranges, service descriptions, units, alarm limits, characterization, etc.

Once I/O tag data is defined, the process control system application functions are configured. This may use IEC 61131 techniques or use configuration methods specific to the control module software. This activity consists of configuration all control functions such as controllers, computation, interlocks, sequences, etc. in each control module, and performing whatever configuration tasks necessary to enable operator view and control of the process data.

7.4.3 Operator Graphics

Configuration activities for operator graphics include such functions as defining a complete and consistent symbol set, including dynamic performance, defining graphics practices such as use of color, backgrounds, alarm behaviors, etc. design of the graphics and navigation between graphics, doing the actual graphics and then fully testing graphics to verify that they are connected to the proper points and that all data and dynamic behaviors are correct.

7.4.4 Reports and Historization

The process control system should be provided with report generation and historization tools that have been tested and certified for use with the rest of the process control system. Third party packages, even if they are commonly used in non-process control functions, should not be used unless the process control system manufacturer specifically endorsed their use. Use of general purpose software may result in loss of function or security.

7.4.5 Independent Device Configuration

Process control systems have many configurable devices, including most field instruments. Configuration and validation of the data must be performed and documented for each of these devices. This consists of simple configuration of smart transmitters, more complex configuration of advanced sensors such as radar or nuclear devices, and programming of independent systems such as PLCs, analyzers and safety systems.

Each of these devices usually is provided with its own configuration and programming software and hardware and may require specialized hand held configurators or PC software and specialized interface data cables. See API 554, Part 3 for a discussion of documentation of configuration data for these devices.

7.4.6 Advanced Control System Programming

Advanced control system programming can be extremely complex and require substantial process testing and development. See API 557 for guidance relative to advanced control systems.

7.5 Software Security

The process control system must allow operating personnel to quickly, efficiently, securely, and safely monitor and control the process, but not allow unauthorized modification of the system or process configuration data.

Certain functions and parameters should be designated as protected in order to prevent unauthorized activity or changes. They should use password features, keylock or special keyboard. Hardware protection such as key locks may be used to provide extra security for SIS bypass or other critical functions.

7.5.1 Security Priority Levels

Access to the system should be protected on a priority basis. The access protection should require programmable password or a keylock. Typical priority levels are as follows:

— *Priority 4*. View only;

— *Priority 3*. Operating;

— *Priority 2*. Supervisory/maintenance;

— *Priority 1*. Engineering.

7.5.2 Security Configuration

It is highly desirable that the security system allow the user to define levels of security based upon user defined general rules and by exception to general rule. For example, a user may chose to allow operator access to low priority alarm settings, but restrict access to high priority alarms to engineering functions. Within that functionality, the user should be able to change the security of a specific point and parameter to one different than defined by the rule. These security rules should be applicable to:

— controller configuration;

— controller tuning or other parameters such as ratios, set point ramp times, etc.;

— alarm settings, individual security setting by alarm type;

— alarm priorities;

— alarm enable/disable; and

— remote access by the system vendor for troubleshooting purposes.

The security system should not interfere with normal operator tasks.

7.6 Reports and Logs

7.6.1 Custom Reports

The capability for the creation of custom reports should be such that all values, measured or calculated, within the system can be accessible for these custom reports.

Process control system software should include an editor to develop custom reports. The editor must be capable of doing custom formats using any of the system database variables. Reports should have the capability to be generated regularly on a timebasis (daily, hourly, etc.).

Reports typically allow export of system data for use in third party reporting systems (spreadsheets, etc.).

7.6.2 Event logging

An event logger should store messages for future reports and displays. The logger should capture the following items as configured by the user (see 8.4.4 for considerations when high time resolution between events is required):

— system events such as errors, module loading, module shutdown and restart, etc.;

— process events such as alarms, changes of state, alarm return to normal and similar events; and

— operator actions such as set point or output changes, controller mode changes, data entry, alarm acknowledgement and horn silence.

An event log display should be provided to display all events logged. The system report generator should be capable of filtering, formatting and printing or storing event records.

7.6.3 Data Historization

The process control system should be provided with the capability to accumulate and store process information history. API 554, Part 1 describes some functional considerations for specification of data historian functions.

7.7 Batch/sequence Control

Batch/sequence functions may be provided in order to perform complex interlocking, sequencing, recipes, and other batch-type applications. The batch functions may be implemented in ladder logic or other types of batch programming language. See ISA SP 88.01 for batch control requirements.

7.8 Communications

7.8.1 Communications Security

Communications security should have error checking procedures with the following minimum requirements:

— error detection and correction on all data transfers;

— automatic retransmission in the event of errors and alarming on a failure after a suitable number of retries;

— continual checking of the back-up communication cable;

— automatic switchover to the back-up communication cable and alarm upon failure of the main communication cable.

7.8.2 Peer-to-peer Communication

The communication system will allow peer-to-peer communication between process control system modules. Such communication should not add more than one second to the processing time (input to output) of any calculation or control utilizing this function. The process control system module should be configured so that if communication is lost, the module will either hold the last value, show bad value, or substitute a value.

The communications throughput should be sufficient to ensure that the operator console is updated to meet stated cali-up time and refresh rate requirements.

7.9 Documentation

The vendor should include a list of the publications that are available and needed for the operations and maintenance of the system. The documentation should be provided in either hard copy and/or electronic format.

7.9.1 System Manuals

The system manuals should describe all the facilities required to implement and modify all configurable system functions at any level of application. Also included should be the following:

— equipment startup/shutdown procedures;

— routine maintenance procedures;

— routine preventive maintenance procedures;

— on-line and off-line diagnostic and testing procedures;

— normal and trouble condition of all diagnostic indicators;

— data backup and restore procedures;

— configuration validation procedures;

— location of all voltage test points and nominal values;

— reference to interpret the meaning of all status codes and alarms;

— site planning, hardware installation and grounding.

7.9.2 Operator’s Manual

The operator’s manual should describe in detail the operator interface and procedures for utilizing all facilities for information retrieval, data entry, and control.

7.9.3 Hardware Manual

A hardware manual should include the following.

— Complete bill of material for all items.

— Statements of system and subsystem functions, of design strategies, and of constraints.

— Description of the hardware configuration.

— Description of operation, including operation of each component board.

— Equipment specifications.

— Inter/intra cabinet cabling drawing(s): all cables are to be referenced by a name and/or part number. All drawings shall refernce cable and conduit schedules.

— Cabling between consoles and cabinets: these drawings shall include pin-out definitions, wiring colors, and cable name/model numbers and all umpers between mounting structures and/or cable termination points.

— Foreign equipment interface cabling: these drawings should include all wiring and connections between the interface devices.

— I/O termination wiring and cabling drawings: these drawings shall include a wiring shedule/drawing identifying each terminal in the DCS enclosure(s) and its connection path to all connections prior to entering an I/O processor. Information on the I/O module name or number, channel, and wire definition (namely, +, –, + power, or shield) shall be included.

— Details of cabinet layouts including dimensions and weights.

— Power supply and grounding requirements.

— Heat dissipation ratings and environmental limitations for all equipment.

— Details of all interfaces to other vendor’s equipment.

— Spare parts information.

7.9.4 Foreign Device Interface

The manual/s for programmable or configurable foreign device interfaces should include some or all of the following depending on the complexity of the interface to the control system:

— design philosophy;

— technical description of the software/configuration;

— language in which the program is written;

— system flowcharts and dataflow diagrams;

— a well-annotated program/configuration listing;

— a description for program linkage, including activation modes, parameters passed, and termination mechanisms;

— a definition of data structures (internal and external) used;

— system utilities for documenting the contents of the system and managing its development;

— software/configuration loading, backup, and downloading procedures;

— software/configuration diagnostic aids, performance monitoring utilities;

— a list of all alarms and messages produced by the software or configuration;

— initialization/restart requirements.

8 Alarm Functions

The most basic function of any alarm is to alert the process operator that a condition exists or an event has occurred that requires operator attention. Alarm systems have the following general functions:

— alert the operator of process or process equipment conditions that require action;

— alert the operator of a diagnostic associated with the process control system;

— alert the operator of other conditions of which the operator needs to be aware of, but do not necessarily require action;

— initiate other event based processes or control actions;

— record events for later evaluation; and

— record events and changes for historical record purposes.

The following section describes a number of functional characteristics of alarm systems. Alarm management issues present a considerable challenge in modern controls systems and are not discussed at length here. See EMMUA 191 for further discussion of alarm management topics.

8.1 Alarm Types

The basics types of alarms are described below. Alarms can be actuated by almost any value that is available in the control system. This could be measured process variables, control parameters, software status, hardware diagnostics or other parameters in the system.

8.1.1 Process Value

Alarm systems should determine when a process value has gone beyond a pre-set condition such as low, high, low-low and high-high. Alarms should be generated if the value is out of range or has failed.

8.1.2 Deviation

A deviation alarm activates when two values differ by more than a pre-set amount (e.g. two separate transmitters measure the same process variable, the controller set-point deviates from the process variable).

8.1.3 Rate of Change

Rate of change alarms activate when a value’s rate of change has exceeded a pre set value. The rate of change may be either a positive or negative value. Rate of change alarms are somewhat difficult to implement as noisy signals

often can give false alarms. Usually some degree of filtering is required to eliminate noise and allow the alarm to function based upon a real trend. Filtering limits the application of rate of change alarms, as the alarm cannot be set to detect rates of change that are faster than the filter time constant.

8.1.4 Discrete Condition

Discrete condition alarms are based upon a value changing to a pre-determined state (e.g. on, off, open, closed, running, stopped, etc.).

8.1.5 Change of State

Change of state alarms are similar to discrete condition alarms, except that there is no pre-determined state at which and alarm occurs. An alarm is activated any time the parameter of interest changes state.

8.1.6 Command Failure

Command failure alarms activate when a commanded action has not had an expected result within a pre-set time limit. They are normally associated with discrete commands such as starting or stopping equipment, opening or closing valves and similar command operations involving discrete events.

8.2 User Defined Functions

It may be necessary to use custom programming to detect alarm conditions that are not available with standard functions in the process control system. Examples would be multiple variable conditions, calculated values, statistical evaluation or parameters that the process control system does not monitor.

8.3 Diagnostics

Diagnostic alarms can vary from alarms that detect a bad process variable, to alarms that detect substantial control system problems. Diagnostic alarms are generated when errors or degraded performance conditions are detected. Normally these alarms will alert the operator of a failure in a control module, input/output module, communications path or other internal state.

Field instrument diagnostics may also be available for some instrumentation. These diagnostics may provide an alert upon detection of a fault, or problems with a process connection. These functions tend to be system dependent.

8.4 Alarm Sequences

Alarm sequences are the actions that occur when an alarm occurs.

8.4.1 Basic Sequence

The basic alarm sequence is as follows.

— The alarm condition is detected.

— An audible alert is turned on.

— The alarm display indicates that a new, unacknowledged alarm exists, usually by changing of color and flashing of a light, display element or a combination.

— The operator may silence the audible alarm by pressing a silence key on a keyboard or other physical device. This will only silence the audible alert and will not change the display of the alarm.

— The operator displays the alarm by accessing an alarm list or graphic display.

— The operator acknowledges the alarm and determines what action should be taken. This silences the audible alert and the alarm display condition will usually stop flashing.

— The alarm display will continue to show the alarm condition as long as the condition exists.

— When the alarm condition no longer exists, the alarm display returns to its normal condition. Usually this is done by changing the graphic display back to its normal color and removing the item from alarm list displays.

8.4.2 Common Alarm Group

The common alarm group sequence, often known as reflash allows a number of alarm conditions to be grouped under one common alarm. The common alarm alerts the operator that one of the items in the group is in an alarm condition, and then the operator must access a separate display or go to an external annunciator or other device to find out what alarm condition exists.

Many process control systems do not have a common alarm group function built into the system and must be built using custom graphics and other system tools.

The common alarm group function operates as follows:

— when any member of the common alarm group goes into an alarm condition, the common alarm point activates and operates according to the basic sequence (see 8.4.1);

— the operator acknowledges the common alarm and it remains in the alarm state until no member of the alarm group is in an alarm state;

— if one or more members of the common alarm group are in an alarm condition, and an additional member goes into an alarm condition, the common alarm point momentarily clears and then returns to an alarm condition;

— when all members of the alarm group are no longer in an alarm condition and the operator has acknowledged the alarm, the common alarm clears.

If a common alarm function is implemented by the user, care must be taken to make sure that when a reflash occurs, the logic driving this function clears the alarm long enough for the process control system to recognize and process the cleared alarm. This is normally a few seconds, but varies with the design of the process control system.

8.4.3 First-out Alarm

First-out alarm sequences are used to identify which of several conditions initiated an event, such as a process shutdown, or equipment trip. The first-out capabilities of a process control system are a function of the specific system and its scanning speed. First out applications must be able to discriminate among several events that may happen almost simultaneously. Many process control systems do not have inherent first out functions, and these must be programmed using other system tools. Typically, the first-out sequence is programmed into the logic solver used to initiate the trip or event based process. The logic solver will communicate this information to the process control system for display and operator action.

There are two basic methods of accomplishing this function.

The first method is the traditional first out sequence. In this sequence the following occurs.

— The conditions that can cause the trip (or other event based action) are configured as a first-out group.

— The initiating condition occurs resulting in a trip that causes other members of the first out group to go into alarm.

— The process control system initiates its alarm sequence for each alarm that occurred whether it was the first to occur or not.

— The process control system flags the first alarm condition that occurred in the first out group and that alarm is displayed in a different manner than the other alarms. This may be a fast flash, a different color, a note or symbol on the display or a combination of these.

— When the operator goes to the alarm display or graphic, it is clearly visible which alarm initiated the event. After the alarms are acknowledged, the first-out condition should still be distinguishable from the other alarms.

An alternate method is as follows.

— The conditions that can cause the trip (or other event based action) are configured as a first-out group.

— The initiating condition occurs resulting in a trip that causes other members of the first out group to also go into alarm.

— The process control system initiates its alarm sequence for the alarm condition that occurred first.

— The alarms that occurred after the initiating condition are masked and not alarmed. Only the initiating condition is displayed and alarmed and all subsequent conditions being logged only.

8.4.4 Sequence of Events

The sequence of events function is used when it is necessary to precisely determine the order of a number of events that may happen almost simultaneously. Process control systems have some inherent ability to perform sequence of events functions, but resolution is limited to the basic scanning frequency of the system. Most sequence of events applications require discrimination of events to less than 1 second and often down to milliseconds. Sequence of events applications with high resolutions may require specialized hardware (e.g. logic solvers). This hardware will determine the sequence of events and communicate that information to the process control system for display and operator action.

The sequence of events function monitors a pre-defined group of points and looks for a change of state or alarm condition of any of the points. When changes or alarm conditions are detected, they are recorded in the order of occurrence. Each event is time stamped to the resolution available.

8.5 Alarm Display Functions

Alarm display functions may be handled by a number of methods as described below.

8.5.1 Alarm Priorities

Any alarm system should have functions that allow alarms to be identified and handled according to their priority. 8.7.1 discusses alarm priority assignments. Audible alerts and alarm displays should differentiate the various assigned priorities, with greater importance being provided for high priority alarms.

8.5.2 Audible Alert

Alarm systems should have an audible alert whenever an alarm condition is detected. The audible alert may be turned off for low priority (informational) alarms. The audible alert style will vary with the needs of a particular installation. The sound level of the alert will depend on the ambient noise level.

The audible alert should have different tones, sound types, or volume levels to differentiate between low priority, high priority and emergency alarms. If there are several operating areas within one central control center, different tones or sound types may be necessary in order to easily differentiate the source of the alarm.

8.5.3 Alarm Assignments

A single process control system may handle more than one operating area. When this is the case, functions must be available to assign alarms to specific operating areas, so that only the alarms appropriate for that area turn on audible alerts and alarm displays.

8.5.4 Alarm Stations

Process control systems may utilize multiple display stations for one operating area. The system design may allow for an alarm to be silenced and acknowledged from any station, or may require that these functions be performed from a primary alarm display station. If the primary station should fail, the system design should allow for another station to be designated as the backup alarm station.

8.5.5 Alarm Display

The process control system should provide a basic alarm display that presents active alarms with the following functions.

— The display should display all active alarms in the system and clearly differentiate between acknowledged and unacknowledged alarms. Time stamps of the times that an alarm occurred, when it was acknowledged and when it returned to a non-alarm state should be either displayed or available for display.

— The display should differentiate among alarm priorities by showing them in different colors, sections on the display or other clearly identifiable method.

— Alarms should be sortable by time stamp, priority, acknowledged or unacknowledged. Typically, unacknowledged alarms are shown first. The default sort should be configurable by the user. Other sorts may be available, but after some time period the display should revert back to its default sort.

— The operator should be able to silence the audible alert from the alarm display.

— When several alarms are displayed on multiple pages or graphic displays. The operator should only be able to acknowledge the alarms currently being displayed.

8.5.6 Custom Graphic Displays

When alarm information is configured into custom graphic displays the following functionality should be considered:

— display the alarm and acknowledgement state of each point on the graphic;

— unacknowledged alarms on a displayed graphic should be able to be acknowledged from that graphic;

— the basic system alarm display should be readily accessible from the graphic or from the keyboard used to access graphics on that display.

8.5.7 Keyboard Linking to Alarm Displays

Alarms and custom graphics that contain alarms should be readily accessible from the keyboard. This is typically accomplished with dedicated keys or hot keys that have been configured to specific displays. These keys may be back-lit or have imbedded LEDs that light or flash to indicate that an alarm exists on the associated display. These

lights may be color coded to indicate alarm severity. Many newer systems use standard PC keyboards and alarm graphics functions to perform this function.

8.5.8 Dedicated Alarm Panels

Dedicated alarm panels for indication of highly critical alarms may be necessary in certain applications. These panels may be driven by the process control system, or independently hard wired. The need for these panels is a function of the hazards of the particular process being controlled or the reliability of the process control system. See IEC 61511 for conditions where dedicated alarm panels may be required.

8.6 Dedicated Alarm Systems

A dedicated alarm system is a stand alone unit which, depending upon local practice, may be required to support critical or safety alarm functions. These systems are also commonly used for local control panels associated with complex equipment such as compressors, fire and gas systems and similar applications. See ISA 18.1 for guidelines for specification of these systems.

An audible and/or visual signal is provided when any one of the alarm points is actuated. This signal will alert the operator to look at the alarm panel to identify the active alarm condition. The alarm point is identified by illuminating a translucent, back-lighted nameplate describing the alarm. Color coding of the windows or alarm lights can be used to identify the priority of the alarm condition or the section of the plant in which the alarm has occurred.

Dedicated alarm systems can be actuated by alarm switches, relay contacts or direct analog signals depending on the type of system. An alarm point can be actuated by an alarm switch that is adjustable (such as a pressure or temperature switch) or fixed (such as for a level switch on a vessel). In some cases, a number of actuating devices may be combined into a common alarm point. Some systems can also accept analog inputs in the form of current, voltage, or direct thermocouple and resistance temperature detector signals. The alarm trip point and dead band are determined by integral adjustments for each input.

Dedicated alarm systems are usually located in the control room and may be mounted on the instrument panel, operator’s console, or suspended from the ceiling. In some instances it may mounted in the field near the equipment being monitored. This configuration could be used for compressors and furnaces to ensure prompt action on the part of field operators. A common-trouble alarm should be provided in the control room. Any field mounted equipment should meet electrical area classification.

Dedicated alarm systems may be capable of:

— outputs via auxiliary contacts;

— output via a data communication link;

— first-out alarms; and

— sequence of events.

8.6.1 Method of Operation

Upon actuation of a dedicated alarm, a light flashes, and an audible device sounds. An acknowledge pushbutton is provided for silencing the audible device and switching the light to a steady-on state. Another pushbutton is provided for testing the alarm lights and, where practicable, for testing the other components of the system.

First-out alarm sequences are recommended to identify the first alarm condition in processes where alarms occur in groups such as alarming the condition that initiated a process or equipment shutdown, which in turn actuated additional alarms as a result of the shutdown.

8.6.2 Audible Indication

Alarm systems, whether dedicated or integrated, require an audible indication to alert the operator that an alarm has been actuated. The visual indication is then used for identification and evaluation.

Audible signals are in the form of bells, buzzers, horns, or electronic devices. These audible signals may be differentiated so that either the location in the process area or priority of the condition.

8.7 Alarm Record Functions

The process control system should log all alarm actions for recall and analysis. The number of events that are recorded before being overwritten should be user configurable and the limits of storage clearly understood. Typically, the number of records is limited only by the memory storage capacity of system.

8.7.1 Alarm Records

The process control system should log all alarm actions such as:

— the time when each point went into an alarm state;

— the variable value at the time it went into alarm;

— when the alarm was acknowledged and the station from which it was acknowledged; and

— when the alarm returned to a non-alarm state.

The system should also have the capability to print this data either to an alarm logger that prints the information as it occurs, or to a system printer from alarm history.

8.7.2 Alarm Data Base Functions

The process control system should have utilities that allow the alarm records to be searched and have data extracted to either paper or electronic reports.

The user should be able to search by time, point number, unit or other process area identification, alarm type or alarm priority. Reports generated with the search utility should be storable for later recall.

8.7.3 Alarm Archive

If the on-line alarm record is limited in size, the process control system should have utilities that allow the oldest data in the record to be archived to removable media for later recall. The utility should include all functions required to recall and search archived information as if it was on-line data.

8.8 Alarm Management Functions

Alarm management functions are very important functions having an alarm system that provides an operator with meaningful and actionable information. EMMUA 191 describes many aspects of this topic and expands upon the basic concepts.

8.8.1 Alarm Priorities

Alarms should be classified according to the potential severity of the alarm condition and how quickly an operator must respond. The process control system should allow for prioritization of alarms and enable different management practices for different priorities. As one example, CCPS identifies the following four alarm priority levels.

— *Level 1*. Alarms that require immediate attention to protect the environment, people or major equipment or to keep a process plant on-stream.

— *Level 2*. Alarms that are important, but of a less critical nature than Level 1 alarms. These alarms may be necessary to maintain processing rate or quality or to protect less critical equipment.

— *Level 3*. Alarms that advise of divergence from normal operation, but which do not require immediate action, or may not require action at all

— *Level 4*. Alarms that are of a minor nature, and which do not require immediate action. These alarms are generally of an advisory nature and often have set points that may be adjusted by the operators.

8.8.2 Alarm Inhibit, Bypass and Disable Functions

Alarm inhibit, bypass and disable functions allow alarms to be turned off because they either not needed, need to be maintained, or are being maintained. These functions can also be used with higher level applications that implement alarm suppression or dynamic configuration. Alarm point may also be configured into process interlocks that effect the operation of process equipment, other control systems or control parameters.

These functions work differently and implementation may vary with the process control systems. The basic functions are as follows.

— Inhibit turns off the audible alert, but the alarm condition will remain on the operator displays. However, the change of state or existence of the alarm is recorded in the alarm history and the status of the alarm point will remain available to the operator through its normal display. Normally, these are general alarms that do not interact with any other control function, shutdown function or process interlock.

— Bypass is used to either maintain or test an alarm point. The audible alert may or may not be turned off and the alarm will be displayed. The bypass should disable any interlocks that effect the operation of process equipment, other control systems or control parameters. There should be restrictions and management procedures for each bypass to insure the integrity of the system and interlocks. The degree of restrictions will be dependent on the nature of the interlocks.

— Disable turns off the audible alert and the alarm is not shown on the operator displays and will not be recorded in the alarm history. All interlocks that effect the operation of process equipment, other control systems or control parameters will be disabled. The alarm can be enabled if it is needed at a later time.

The process control system should have functions that allow a summary of all inhibited, bypassed or disabled alarms to be viewed from one display with a printed report available. The ability to inhibit, bypass or disable any alarm point in the process control system must be controlled by operating restrictions and procedures. Any changes to the existing system will require a management of change procedure.

8.8.3 Dead Band and Delays

Dead band and delays allow alarms to be configured so that they do not clear and re-alarm when the alarm condition is oscillating around the alarm point.

Dead band is used for alarms based upon continuous values, and requires that the value being monitored move to some value beyond the alarm setting before the alarm will clear. Dead band is usually expressed in a percent of the alarm set point, but may also be expressed in process units.

Delays are generally used for alarms based upon discrete points. Once a discrete point goes into an alarm state, the alarm will not clear until the point has gone into a non-alarm state for some pre-determined period of time.

8.8.4 Alarm Suppression

Alarm suppression is a function that prevents an alarm from becoming active under pre-defined conditions. Normally, suppression is applied to reduce the number of alarms that one event will generate. For example, a pump shutdown might generate an alarm and at the same time suppress low flow and discharge pressure alarms.

Some process control systems provide functions that allow the user to define conditions under which alarms are suppressed. These functions are fairly simple and allow for suppression under a limited number of conditions. When this function is available, there should also be a detail display that is accessible from the alarm display that allows the operator to readily view the alarms that are being suppressed and what their statuses are.

Other process control systems do not have inherent suppression capabilities, but have general programming functions that allow the user to build custom suppression functions by accessing inhibit, bypass and disable functions of the alarms. In these applications, the user is responsible for developing detailed displays that will show the operator what is being suppressed and why.

8.8.5 Dynamic Alarm Configuration

Dynamic alarm configuration is a function by which a large number of alarm settings, priorities and actions can be modified based upon an operating state of a process. This function is not used to great extent in continuous refining process, but is often used in chemical and pharmaceutical batch processes. In this application the alarms that are required, their settings, actions and priorities change as a plant moves through its various operating phases. Dynamic alarm configuration functions allow these conditions to be pre-defined and applied to the affected points automatically as the process goes through its various phases and steps. ISA S88.01 discusses application of dynamic alarm configuration to batch processes.

8.8.6 Management of Change (MOC)

MOC functions prevent changes to key values from being made by unauthorized personnel and provide a record of significant changes that are made to the alarm system. Some MOC functions are as follows.

— The process control system should be configured with different security levels. The security level for each alarm point should be determined by the functionality of the point. For example, low priority alarm set points may be changed by an operator or operating supervisor, while high priority alarm settings must be changed by the operating department supervision.

— The ability to inhibit, bypass or disable high priority alarms should be determined by required security level.

— All changes in alarm settings, priorities, and the inhibition or disabling of alarms, when they were changed, what they were changed to and who made the change will be recorded and documented per operating department procedures.

8.8.7 Alarm Management and Evaluation Tools

The increasing sophistication and number of alarms available with process control systems requires functions that allow analysis of the alarm system performance and enforcement of alarm policies. Some alarm management and evaluation functions are listed below. See API 554, Part 3 for management of change discussions.

— Monitoring alarm settings for critical alarms against a master list of authorized settings in the alarm management database. This function may generate reports of alarms that do not match the authorized settings, or may have the capability of automatically reset alarm settings to the approved values.

— Monitoring of alarm inhibit and disable statuses against approved states for critical alarms. This function works in the same manner that the setting monitor works. It could either generate reports of non-conforming points or be set to automatically enable the alarms.

— Data collection and analysis of alarm performance metrics such as the number of alarms active, alarms per hour, chattering alarms (alarms that turn on and off regularly) and alarms that occur for each operating crew. This data can be used to identify alarms that have no value, are not operating properly, or to identify problems in operating procedures and practices.

8.9 Documentation

A complete and accurate record of all alarm setpoints should be maintained. This record should include tag number, service description, alarm setpoint, priority, basis for the alarm setting, dead band, and P&ID or loop-drawing numbers.

9 Interlocks

Interlocks provide corrective actions and/or process shutdowns to protect equipment or reduce undesirable product quality. These systems may be part of the process control system or stand-alone equipment and they sense process conditions, generate alarms, and manipulate devices such as control valves, motor starters, or other control devices.

9.1 Types of Interlocks

Interlocks are used for equipment protection and process control.

9.1.1 Safety Instrumented Systems

Safety instrumented systems are outside the scope of this document. Their design and implementation are defined by ANSI/ISA 84.00.01.

9.1.2 Equipment Protection

Equipment interlocks are prevent damage to process equipment such as compressors, motors, gearboxes, pumps, turbines and other rotating equipment. This could include equipment monitoring systems for vibration, temperature, lubrication or other measured variables.

9.1.3 Process Control

Process interlocks are usually performed within the process control system and are used to control continuous and batch processes from start-up through shutdown. They prevent lost production and maintain product quality. The logic can be simple or complex depending on the application.

9.2 Sensor Considerations

Transmitters are preferred to switches and/or relays. Transmitters produce a variable signal and have some built-in diagnostic capability. A switch or relay will produce a discrete signal and will require testing to determine operational status.

Asset protective system sensors must be highly reliable. Sensors may be switches or transmitters. Critical protective systems should consider redundant sensors to meet system reliability requirements. Consideration should be given to trouble shooting, calibration, and ease of replacement of sensors. To achieve reliability, an independent, direct-connected sensor is employed to monitor the measured variable and initiate the automatic action. Such a device is not dependent on any other piece of equipment or system for its function. This sensor should be connected independently to the process and not share impulse piping or valving with any other device.

The sensors are typically applied in a de-energize-to-trip configuration such that automatic action is initiated upon sensor, signal, or power failure. If energize-to-trip systems are installed, more frequent scheduled testing may be required. Some specialized applications, such as NFPA fire and gas installations, may utilize energize to trip functions, but these applications require circuit integrity monitoring and alarming.

9.3 Shutdown Alarms

All shutdown initiating functions should also be annunciated to determine the cause of the event. For complex interlocks a first-out alarm display or sequence of events report should be used to identify what caused the shutdown.

9.4 Pre-shutdown Alarms

A pre-shutdown process alarm enables the operator to take corrective action before the shutdown is activated. They should be used when practical.

9.5 Testing

Interlocks should be inspected and tested on a scheduled basis. Trip systems that can not be tested during operation should be scheduled during planned shutdown.

Bypass systems should be considered when on-line testing is required. When any bypass is in effect it should be annunciated in the control room. It is recommended that only one input or output is bypassed and tested at a time. The alarm circuit/s for a bypassed function should remain operational.

9.6 Documentation

Interlocks should be documented, including configuration, logic documentation complete with annotations, operating, testing, lockout and maintenance procedures. There should be an administrative process to approve and document set point and logic changes.

10 Data Management and Documentation

Documentation for process control systems is complex and extensive and requires rigorous management. The advances in application of digital technologies to all parts of a process control systems also has resulted in a great amount of the data being automatically generated and stored in digital forms.

Figure 3 in API 554, Part 1, repeated here illustrates the types of data that its typically necessary to operate and maintain a process control system. This data illustrates only that data necessary for the process control system and does not cover the extensive interfaces required to other business systems, nor does the figure attempt to define how these data functions are implemented.

The figure shows an overview of the data systems that should exist in a facility. The exact design and implementation of these functions will vary from site to site and depend greatly upon site practices, staffing, organization and policies. However, many of these systems are application specific, may be proprietary (or partially so) and attempts to integrate these specialized functions have resulted in failure or substantial loss of functionality and flexibility. Each of these functions and typical implementations are described below.

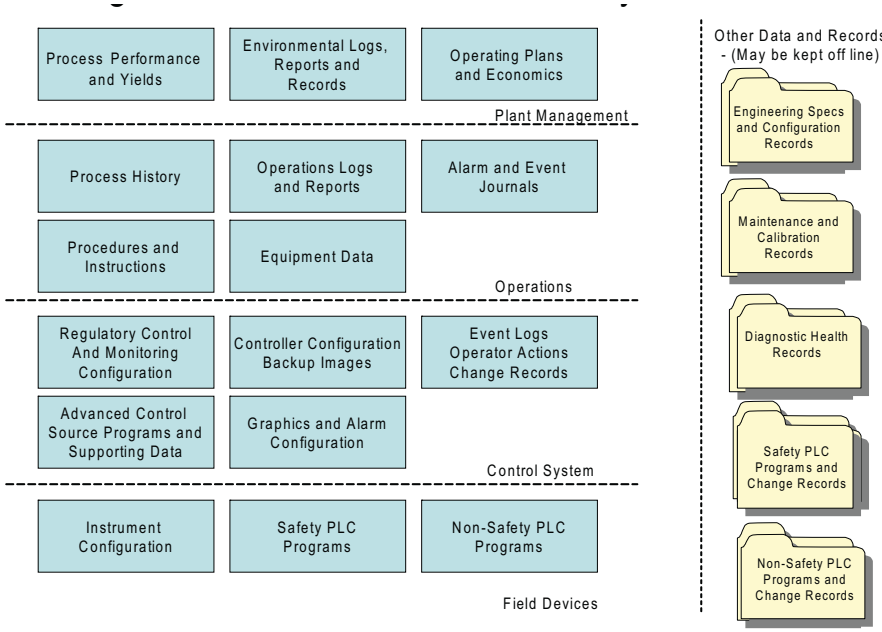

Figure 4—Process Control System Data

10.1 Field Instrumentation

Modern field instrumentation contains microprocessors and significant amounts of memory. Each instrument holds its own configuration data which defines the function of the instrument and also provides local diagnostic and set up support. This data is downloaded from various programming tools, usually a hand held device or PC. The data is resident in the device, but records of the data need to be kept separately to provide backup and a data source to reload the field instrument configuration when it is repaired or replaced.

10.2 Field Instrument Asset Management Systems

Field instrument asset management systems are available from a number of sources, usually from major process control system manufacturers or companies that specialize in instrument calibration systems. These systems are very specific in their functions and must be readily adaptable as new instrumentation and functions reach the market. These systems may have some or all of the following characteristics:

— capability to create instrument tags and associate configuration data, calibration requirements or other tag specific design data;

— interface with recording calibrators to download calibration procedures, routes and calibration specifications to upload as-found/as-left data;

— capability to communicate directly with instrumentation either via a direct PC connection or via network connections and interface multiplexers and to upload and download configuration data and monitor device diagnostics and error messages;

— the ability to store device (model, serial number, software version, etc.) and configuration data for smart instruments and provide audit trail functions on configuration changes;

— capability to export data to external systems or databases using standard data transfer tools;

— capability to integrate with special purpose software tools such as smart valve positioner, complex instrument or similar external software; and

— capability to have additional or updated devices added to the list of devices that the application is aware of and for which data can be captures.

10.3 Process Control Systems

The data captured by or retained by process control systems has been extensively discussed in this document. Also see API 554, Part 1, Section 4 for a discussion of the various types of data that are contained in the process control system.

10.4 Other Specialized Systems

There are a number of special application data base systems that are available for specific applications and equipment. These data functions are usually very specific to the type of application and usually cannot be integrated with other data functions. These applications include the following.

— *Machinery monitoring systems*. These systems are used to collect very high speed data from machinery vibration monitoring systems and provide complex analysis of machine behavior.

— *Analyzer monitoring systems*. These systems are used to monitor the behavior of process and environmental analyzers. Functions may be highly varied and include automatic calibration, analysis of spectra or gas chromatograph (GC) column output signals, or data capture and model development for near infrared (NIR) or other correlation based analyzers.

— *Environmental monitoring and data systems*. These systems may be general purpose data applications that are segregated for purposes of collecting and reporting of data that shows environmental or other operating permit compliance.

10.5 Engineering Database Systems

Engineering data base systems provide a platform for the design and engineering for process control systems in both a project environment and in a plant as-built data base maintenance environment. The engineering system typically provides the following functions:

— management of loop and tag numbers;

— specification forms (data sheets) for individual instruments;

— wiring specifications and interconnections;

— wiring reports by cable or terminal box;

— loop diagrams;

— instrument index;

— segregation of project and as-built data;

— utilities for import of project data into the as-built database; and

— functions to support configuration of process control system tags.

Engineering data bases take a variety of forms. The simplest, and usually least effective are little more than spread sheet based specification forms. More sophisticated systems provide complete engineering platforms, including modules or interfaces that support common sizing calculations.

Some facilities still operate based upon paper drawing systems, or even CAD based drawings, but which are not integrated with data. These systems are generally inefficient and result in lost data and poor coordination of engineering updates.

Engineering documentation systems must provide for work processes that allow for effective and efficient management of project engineering for existing facilities and accurate and timely integration of completed engineering projects into the as-built documentation system. This process requires that either the engineering data base application allows for simultaneous engineering and as-built work to be done, or provides a means of simply and accurately importing of project data.

Many engineering database applications have poor facilities when it comes to coordination of projects and as-built data, and require considerable manual work and resources to provide that coordination. Typically, these systems fail because the resources are not available to provide the needed coordination and data maintenance.

10.6 Maintenance Management Systems

Maintenance management systems are used for a variety of functions required to maintain process equipment. Among these general functions are as follows.

— Retention of basic specification data for equipment.

— Retention of process locations and equipment that is installed at each process location.

— Maintenance of spare parts lists for mechanical equipment.

— Management of work processes including work orders, labor and material costs and work order feedback.

— Management of labor loading and scheduling necessary for execution of work orders.

— Procurement functions including purchase requisitions, purchase orders and receipt and use of material records.

— Management of spare parts inventories.

— Equipment repair history and failure tracking.

— Equipment location history.

— Failure and repair history analysis.

— Integration of maintenance costs into higher level financial management systems. In some applications, the maintenance management functions are integrated with the larger financial and planning functions.

Historically, maintenance management systems have been successfully applied to mechanical equipment such as pumps and compressors, process vessels and tanks and pressure relief valves. In even a large refinery or chemical

plant, the quantities of this equipment is limited to several hundred pieces of equipment and several thousand pressure relief devices. Furthermore, the data handled by the maintenance management system is relatively limited and static. For example, mechanical equipment and pressure vessels tend to be installed and have limited and infrequent modifications over long service lives.

Maintenance management systems structured for mechanical equipment and pressure containing equipment have not had successful application to process control system functions. The reasons for this are as follows.

— The quantities of instrumentation and control entities that would have to be loaded into and tracked by these systems are 2 to 3 orders of magnitude higher than the numbers of equipment. For example, a facility that has 1000 pumps, compressors, vessels, etc., may have 100,000 to 400,000 instruments.

— The data required to define an instrument or process control system component is often much more complex than required for a piece of mechanical equipment.

— Instrumentation and process control system components have a substantial amount of configurable information contained in them.

— Many modern instruments and process control system components are capable of being monitored while in service and generating a variety of alerts and diagnostics.

— The data handling requirements of instrumentation and process control system components are extensive and highly variable. The data and its format is usually quite different from component to component and manufacturer to manufacturer (and often varies within a manufacturer's lines as new lines and updates are introduced).

— Instrument and process control system components are subject to frequent modifications and/or replacement. Usually this replacement results in a significant change in the required data that must be tracked (e.g. a replacement has different or more configuration data, increased diagnostic data available, etc.).

General purpose maintenance management systems do not provide the flexibility to support all of the variations in instrument and process control system data, nor are they generally flexible enough to accommodate the frequency and quantity of data changes. This results in a need for a number of special purpose instrument and process control system applications to work in coordination with the maintenance management systems. Figure 4 shows a typical set of these applications. The interfaces with the maintenance management system and the underlying instrument and process control system are generally as follows.

— The maintenance management system is used to maintain general information on instrumentation and process control system and to track work orders, costs, purchases, etc. It also is the primary source of general information for maintenance management personnel, but is not intended to provide all details necessary to maintain instrumentation and process control system components.

— The engineering data base system is the source of instrument and process control system tag (locations) and specification information (e.g. datasheets). The basic location, service description, etc. information should be automatically passed to the maintenance management when changes to the as-built engineering database occur. Some basic specification information may also be passed.

NOTE In small plants, this may be practical to management manually, but this places a permanent burden on staffing.

— The instrumentation asset management system provides the means of keeping configuration, calibration and diagnostic information. Instrument specific data such as manufacturer, model, serial no, software version, etc.

could be pushed to the engineering data base and maintenance management systems as determined by work practices. Calibration data may also be pushed to the maintenance management system.

— Specific maintenance event data such as inspection, test and repair details could be kept in the engineering data base system, asset management system or maintenance management system. However, this data is generally extremely type specific and is usually too complex for general maintenance management systems to accommodate. Typically, this data is kept in type specific records in the engineering database or asset management system and general data (e.g. a repair, calibration or test was performed) is passed to the maintenance management system.

— Diagnostic alerts generated by the asset management system may be passed to the maintenance management system in order to automatically generate a work order to check the instrument or process control system component.

10.7 Process Data Management Systems

Process data management systems include all functions required to acquire, store and report process data historical data. These functions are discussed in API 554, Part 1. These functions are typically implemented in process historian data collector computers which reside on the process control network. These data collector modules then pass their data to a historian module that stores process data, including events such as alarms, changes in status, etc., and provides it to data consumers as needed.

The data consumers are typically advanced control applications, desktop data access or data collection for yield accounting or other business management functions that rely upon current or historical process data.

Usually, the primary process data collectors and historian modules reside upon the process control network, and communications to the business network must be secure. This is usually accomplished by use of a DMZ and a shadow database on the business network. See 4.6 for a discussion of this architecture.

10.8 Data Integration

As described above, there is a substantial amount of highly specialized data associated with process control systems that originates in, or is held by, a variety of independent and specialized applications. Also in practice, these functions are far too specialized and dynamic to expect that any general purpose application could handle the functions, or keep up with the continuous changes that occur continuously in the process control system environment.

Numerous organizations offer commercial data integration solutions in a variety of forms. These applications generally have the characteristics listed below.

— The data integration application is usually a centralized database that resides on a business network and has the capability of receiving data from various sources and distributing it to applications that need the data.

— Each piece of data that is contained in the integration system has a defined source and list of data users. This is a critical and often difficult part of the specification and design as the users must understand the philosophy of what data is required by various users.

— As data is generated by the data suppliers (new or revised data), the data integration system either reads the data, or has it pushed by the source application and stores it in the data integration database. Some source applications are capable of pushing data, and some are not.

— When new data is stored in the data integration application, it either distributes the data to applications that need it, or supplies the data upon demand.

While data integration packages are marketed as an application, implementation in a given situation usually requires substantial design and implementation work, and may require some level of customization. While the application may provide the data structure and data interface capabilities, the data and its use must be clearly and succinctly defined.

The means of user interface and reporting must also be defined. For example, the maintenance management system may be the primary way that general users obtain information. In this case, the amount of data that the maintenance management system needs to access and format may be significant.

A common use of the data integration application is to provide users with a common interface for many applications. In this case, all data is held in the data integration application and suitable reports and information displays must be defined for the system.

11 Instrument Power Systems

The process control system electrical power supply and distribution design is an important factor to the reliability and availability of the control system. This document covers the requirements for the process control system only; it will not cover power requirements for process equipment. For additional details see PIP PCCEL001, *Instrumentation Electrical Requirements*.

11.1 Process Evaluation

The response of the process to partial or total power interruptions must be evaluated to determine control system power requirements. The following considerations will determine if the control system must continue to function during power interruptions.

— How will the process shut down when power is lost to the primary process drivers and energy input devices?

— What exothermic reactions or other processes that could result in overpressure, over temperature or other unsafe conditions if power is interrupted?

— What are the economic considerations of a power interruption?

— Can the process be readily and quickly restarted after power is restored?

— Can the inventory contained in the process be used if the process is restarted or is it ruined?

11.2 Control System Evaluation

The response of the control system to partial or total power interruptions must be evaluated. Some considerations are as follows.

— What is the response of the control system to primary power loss?

— What is the response of the control system to a power dip?

— What is the response of the control system when power is restored?

— Is a software and data reload or recovery required when power is restored?

— What field instrumentation can tolerate a power interruption?

— If backup power is required, how long will it be required?

11.3 Instrument Power System Design

Once the process and control system power requirements have been identified, an overall electrical power system design is developed.

The following design considerations are described in the paragraphs below:

— process control system power source;

— AC power distribution;

— AC power distribution to external powered instruments;

— DC power supplies;

— redundant DC power supplies; and

— DC power distribution.

11.3.1 Power Source

The primary power source for all process control systems is supplied from a public utility or internal plant generation system. Does the primary power source meet the availability and reliability requirements for the process control systems? If not, additional design considerations should be evaluated.

Some examples to increase availability and reliability of the primary power source are:

— double-ended electrical substations;

— emergency generators;

— static transfer switches between two power sources; and

— UPS.

The process control system power source generally must have high availability and reliability, because it powers the operators interface to the process. This would include the DCS, PLCs, analyzers, alarm systems, field instrumentation, information systems, interface to motor controls and other systems. These systems should be powered from a UPS system that can provide back up power for a minimum of 30 minutes. Care must be taken in the design of the power source to the DCS to avoid a single point of failure causing loss of control.

Not all process control system equipment requires secure power, such as printers or similar equipment may be powered from utility power.

The use a centralized UPS or distributed multiple UPSs will be dictated by the process control system topology. The decision to power a remote location from a centralized power system should consider factors such as distance and exposure of the power wiring to fire or mechanical damage.

11.3.2 AC Power Distribution

The primary power source typically supplies 480 VAC through transformers to provide 120 VAC to the AC power distribution system. This would typically consist of UPS system/s and instrument panels. The UPS system/s would supply power to critical instrumentation and control systems. Instrument panels would supply power to non-critical instrumentation, control systems and other supporting equipment (i.e. radio systems, computers etc.).

The distribution system should be designed to accommodate maintenance philosophies and future plant expansion. Each DC power supply should be individually protected using coordinated fuses and/or breakers. Branch circuits serving DC power supplies should not be shared with other electrical equipment. These loads can induce unacceptable noise and electrical transients into the power system (i.e. fans, power tools, welding machines, etc.).

All panels should be properly labelled to identify the load on each circuit.

11.3.3 AC Power Distribution to External Powered Instruments

Many field instruments, particularly in-line flow meters, analyzers or other special purpose instruments require external AC power. Depending upon the application, this power may come from a UPS or AC power distribution panel.

11.3.4 DC Power Supplies

DC power supplies are used to provide power to:

— process control systems;

— 2-wire loop powered instruments; and

— external instruments.

Power supplies for process control systems serve two purposes. They supply power to the electronics that operate the control system and feed field instruments (analog and digital) through the control system rack bus arrangement. These power supplies can be integral to the control system or external depending on the manufacturer or control system architecture.

Devices that require more power than available from the I/O modules require an external power supply such as solenoid valves, 4-wire DC instruments and 3-wire instruments (i.e. gas detectors).

Power supplies should have over-temperature protection and integral fuse protection. Critical power supplies should have a loss of power alarm connected to the process control system to inform the operators of a failure. It is permissible to “daisy chain” or “series” several related loss of power alarms together to activate a single “common trouble” alarm for a group of power supplies. These power supplies should have status LEDs to indicate which power supply caused the common alarm.

11.3.5 Redundant DC Power Supplies

Redundant power supplies should be used in applications where the control function is required to operate when the power source has failed or to meet integrity requirements of the process. The system should accept power from two different power sources, one of which should be a UPS. Power supplies should be replaceable on-line without disrupting the process and without impacting control capability.

Redundant power supplies should have a loss of power alarms that are connected to the process control system or other operator interface. There shall be one alarm per power supply and the alarms shall be wired in a failsafe manner. If the alarms are not built into the power supplies, then supervisory relays shall be installed on the output (DC side) of the power supplies to provide loss of power alarms.

11.3.6 DC Distribution

Provisions should be made to distribute DC power from the power supplies to the required loads. This can be done using circuit breaker or fuse panels. These panels must be designed so that a short, ground or other fault in the field instrument or its wiring affects only that instrument and does not cause a failure of multiple inputs. It is recommended

that the DCS or source instrument either be designed with current limiting circuitry or fuses to protect the instrument and other input channels from a field instrument or wiring fault.

Power wiring for field instruments, two-wire analog transmission loops, field switch contacts, etc., should be individually fused and provided with a means of disconnecting the power without disturbing terminated wiring (e.g. knife-switch type terminal blocks). Visual indication of a blown fuse condition should be considered to trouble-shooting. Wiring connected to I/O modules or source instruments containing individual current-limiting circuit protection does not require fuses. Low level signal wiring connected directly to I/O does not require fuses. Low level signals are defined as millivolt, microamp, pulse and frequency signals less than 1 volt.

If a single circuit is used to distribute power to multiple loops or components, proper identification shall be provided at the distribution source listing the effected devices.

11.3.7 UPS System Design

For details on UPS system design see PIP ELSAP03, *Design and Fabrication Ferroresonant Uninterruptible Power Supply (UPS)*.

Sizing of UPS applications for process control system applications can be complex as numerous factors need to be considered.

— UPS reliability and robustness must be carefully evaluated. Usually, multiple parallel smaller UPS systems are desirable instead of one large system. The UPS load distribution should be evaluated to ensure that failure in any UPS will not cause unacceptable failures of the process control system.

— In many process control system applications, there are often redundant power supplies. It is recommended that these supplies be powered from two UPS units rather than from a single unit. This can result in several UPS load cases when different combinations of power supply failure and load sharing functions are considered. When parallel UPS applications exist, the failure of one UPS and the accompanying load shifts to the other UPS must also be considered.

— The characteristics of process control system power supplies must be considered in specifying the UPS. Many of these power supplies have non-sinusoidal load curves which affect the UPS sizing criteria.

— Process control system power supplies also can have substantial inrush loads when they are started. While it is impractical to size a UPS for inrush loads for all connected loads, some fraction of inrush must be allowed for.

— Local codes may require the UPS to be sized for all connected loads. This becomes an issue when load sharing occurs in redundant applications, or when an oversized power supply relative to the process control system power demand is used. In these cases, local codes may not allow for consideration of actual demand vs. rated load.

12 Electrical Considerations

12.1 Grounding

Electrical systems must be connected to ground for the protection of personnel and equipment from fault currents (AC safety ground) and to minimize electrical interference in signal transmission circuits (instrument circuit ground). Consult manufacturer’s recommendations for process control system equipment grounding requirements. For additional information on electrical grounding, see NFPA-70, Article 250, API 552, API 540 and PIP PCCEL001, *Instrumentation Electrical Requirements*.

12.2 Electromagnetic Interference

Electromagnetic interference is the result of any spurious effect produced in the circuits or elements of electronic equipment by an external electromagnetic field. Electronic equipment can be susceptible to interference from nearby sources such as power transformers, radio/television transmitters, cellular phones, pagers, PDAs, and electric motors. A common source of interference is from portable radio transmitters, particularly when used in the immediate vicinity of the electronic equipment rack. Electromagnetic interference can introduce message or signal transmission errors. Warning signs should be placed on entrances to rooms housing sensitive equipment.

For additional information on electromagnetic interference, see API 552.

12.3 Signal Wiring Systems

The design of signal wiring systems should conform with local jurisdiction codes and owner standards and practices. Signal wiring systems generally consist of the following major components:

— field instrument terminations;

— individual pairs or other wiring connections to terminal boxes;

— local terminal boxes;

— cables or other conductors from local terminal boxes to marshalling panels;

— marshalling panels;

— cables or other conductors from the marshalling panels to process control system I/O terminal panels; and

— process control system I/O terminal panels.

The overall design of the signal wiring system should define requirements in the following areas:

— overall wiring philosophy including use of marshalling panels, overhead vs. underground routing and signal separation requirements;

— cable and wire specifications for all signal types (e.g. 4 mA to 20 mA, thermocouple extension wire, low voltage wiring, serial communication wiring, fiber optic etc.);

— installation requirements—use of conduit vs. cable tray, support and routing requirements, etc.; and

— wire naming and labeling conventions.

See API 552 and PIP PCCEL001 for further guidance.

12.4 Communications

The greater use digital communications requires that the design of these systems receive greater attention. Communications wiring should be classified and requirements for each classification defined. General classifications are as follows:

— fieldbus communications;

— complex instrument communications (e.g. RS-485, Modbus, HART, etc.);

— control and information network communications; and

— business LAN communications.

The wiring design requirements for these systems will vary with the application and must be appropriately defined with due consideration to the integrity required by the application. Typical wiring types used are as follows:

— shielded twisted pair—fieldbus and complex instrumentation communications;

— shielded multiple wire—complex instrumentation communications;

— unshielded multiple pair—ethernet Cat 5 and Cat 6 cable used for control and information and business LAN; and

— fiber optic—used for almost any communication system where extended distances, immunity to electromagnetic interference, or isolation of communication segments are required.

It is highly recommended that overall system diagrams showing all communications and type of wiring that is being used be prepared. This diagram should also show all communications support equipment such as routers, switches, hubs, patch panels etc.

The communications systems design should also address separation of functions and define where networks may or may not share cables, communications hardware, etc. For example, the separation of business LAN and control and information network communications is usually a critical item as they often share the same communications technologies, but separation of the two systems is usually a requirement.

13 Control Centers

The discussion in this section addresses functional requirements that are unique to the design of control centers. These design requirements must be coordinated with the building designers in order to assure that the physical building will meet the needs of the business. This section does not address building construction or architectural design.

13.1 General Considerations

A control center is a facility from which the control of a process plant or plants is coordinated. The primary function of a control center is to accommodate the necessary operations and process control personnel and the process control operator stations and displays to provide safe, continuous operation of the process plant(s).

The process control operator should be provided with control stations that display the process plant operating data.

The actual process control equipment that processes and controls the input and output signals may be located in satellite buildings or field locations. Digital and analog data transmission technologies and communication systems make this practical and cost effective. Therefore, more than one process plant can be controlled from a single control center.

Some of the factors which should be considered include the following:

— the type of control equipment to be housed;

— the number of process units to be controlled and how control is to be integrated;

— the location of the building;

— the environment in which the building will be located;

— the environment within the control center;

— any requirements for future space;

— office requirements;

— maintenance space and spare parts storage;

— facilities for personnel;

— personnel and equipment protection;

— personnel ergonomics and noise;

— handicap access; and

— equipment spacing.

13.2 Control Center Site Selection

Control center site selection should consider the factors listed below.

— The distance from processing units and potential overpressure from the effects of a process incident. In general, these requirements are based on the *National Electrical Code* NFPA-70 and API 500. Other documents such as the Dow Safety Index are commonly used in assessing control center siting and construction requirements.

— The potential for exposure to release of materials that could affect the health and safety of personnel who work in the control center.

— The number of personnel that will be housed in the area and traffic of personnel in and out of the area.

— The number of units that will be operated from the control center, their relative locations and relative process relationships.

— The elevation with respect to drainage, flooding, and spills.

— Prevailing winds.

— Locate in a non-hazardous electrical classified area.

— National and local regulations.

13.3 Physical Design Criteria

The physical design of the control center should meet the following minimum requirements:

— should meet all local building codes and standards;

— should be constructed of fire resistant building materials;

— should avoid the support of roofs by non-ductile walls;

— should have suitable laboratory testing area if required;

— should not have connections inside the building to process sewers or storm sewers;

— should not have external windows unless the control center is located remote from blast areas; and

— should not have hazardous or ignitable liquids or gases routed into the control center.

The control center may need to be blast resistant to protect personnel and control and process computer equipment to allow for the safe and orderly shutdown of the process at the time of an incident. See PIP STC0101A, *Blast Resistant Building Design Criteria* for detailed information.

13.4 Control Center Building Design and Layout

Control center building design and layout is determined by the number of process units to be controlled from one location and the amount of equipment and personnel that will be in the center. The control center should be designed to accommodate future expansion. The following key areas should be considered:

— control room;

— process control system equipment room;

— instrument/electrical maintenance room;

— communications systems room (i.e. telephone, IT equipment, radios, etc.);

— HVAC/mechanical equipment room;

— UPS/electric utilities room;

— battery room; and

— safety equipment storage.

The following auxiliary areas may be considered:

— kitchen and eating area;

— locker, changing area, restroom and shower facilities;

— offices;

— conference room;

— training/process simulator facilities; and

— laboratory facilities for operator performed testing.

13.5 Control Center Environmental Controls

This section presents some practices and considerations for the selection of environmental equipment.

13.5.1 Heating, Ventilating, and Air Conditioning (HVAC)

When designing a system for a control center, the following load factors should be considered:

— inside design conditions;

— outside design conditions;

— size and physical characteristics of the control center;

— average number of occupants and degree of activity anticipated;

— heat load from the equipment housed in the control center, including provisions for future expansion;

— quantity of air assumed for ventilation and leakage through doors, windows, and wall penetrations;

— manufacturer's site planning guides for the installed equipment;

— positive pressure design; and

— redundancy.

Consideration should be given to potential problems caused by HVAC system failure. Redundant systems should be considered to prevent serious overheating of electronic equipment.

13.5.2 Air Purification

In addition to providing for human comfort, air purification should be considered to protect the instrumentation in the control center against corrosion, abrasive particles, conductive particles, and potentially hazardous fire or explosion conditions. Air purification includes the following items listed below.

— Filtering suspended particles using either fiber or electrostatic-type filters.

— Removing corrosive vapors (such as hydrogen sulfide, sulfur dioxide, and ammonia) by providing a filter system with an absorption media. (Refer to the ASHRAE Handbook or filter manufacturer's literature for information on the selection of the equipment and filter media required for specific applications.) Manufacturer's site planning requirements and recommendations should be consulted.

Fresh breathing connections or other air breathing devices should be provided to support the minimum number of personnel who must remain in the control center during emergency conditions. A centralized breathing air system that provides at least one hour of breathing air to each control console is recommended.

Refer to Standard ISA-S71.04, *Environmental Conditions for Process Measurement and Control Systems*: *Airborne Contaminants*. It is suggested that for computer and microprocessor-based equipment, gas concentration should be limited to the G1 severity level (mild). For other instrument systems the G2 severity level (moderate) may be acceptable.

13.5.3 Positive Air Pressure Systems

A positive air pressure system for a control center is used to prevent the entry of flammable and corrosive atmospheric vapors or gases when the control center is located in an electrically classified area. This is usually accomplished with a positive pressure ventilation system using a clean air source in conjunction with effective safeguards against ventilation failure. NFPA 70 and NFPA 496 address the criteria to meet hazardous area requirements. An air lock entry door system will minimize loss of pressurization and ingress of contaminates.

The source of air for positive air pressure systems in control centers should be free of flammable vapors, gases, corrosive contaminants, and other foreign matter. Combustible or toxic gas detectors may be required on the air intake to indicate when these gases are present. An alarm should be generated when concentrations rise above normally expected levels and automatically close inlet air flow to the building.

Locations of air intakes are determined by the nature of the process and the physical layout of the plant. Ordinarily, the fan suction should be taken from an area to the side of the building furthest from the process area with the intake opening at an elevation where the electrical classification is non-classified 30 ft (9 m) above the surrounding plant grade minimum. The air intake should be fitted with a bug screen.

13.6 Control Center Lighting

Lighting has a significant impact on the efficiency, comfort, and general effectiveness of the control room operator. Operator displays require special lighting provisions and controls. Lighting fixtures should be arranged and the surrounding environment selected to ensure that glare is minimized.

The lighting level behind the control panels or in equipment rooms depends on the type of instrumentation, the type of equipment, and the maintenance activity anticipated in the area. Harsh, exposed lighting should be avoided.

An emergency egress lighting system may be required and should meet appropriate building codes.

13.7 Floor Design

An access or computer-type floor is recommended for use in rooms with electronic instrumentation. This type of floor simplifies the routing of cables between process control equipment, auxiliary equipment and operator consoles. The use of under floor cable trays may be considered for organized routing. A floor height of 18 in. to 24 in. (0.5 m to 0.6 m) from the concrete sub floor to the top of the floor is recommended. The concrete sub floor should be above grade.

Floor drains should, as a minimum, be in accordance with applicable building codes. Such drains should be provided in areas where moisture could accumulate at low points. Drains should be provided with adequate seals and be connected to the appropriate drainage systems. A water detection system may also be necessary.

13.8 Control Center Fire Protection

The fire protection system shall be in accordance with the NFPA 497A, *Fire Protection Handbook* and the applicable local codes and ordinances.

For rooms with raised floors the following system should be provided:

— a system of ionization and optical smoke detectors with audible and visual alarms; and

— portable extinguishers suitable for indoor electrical fire service.

A fire alarm control panel (with backup battery supply) should be provided which shall be capable of performing the following:

— sound alarms throughout the protected area;

— shut down the air-conditioning and close fire dampers;

— activate an audible alarm in the control panel until the fire condition is fully actioned;

— report on any fault in the detection system and provide audible and visual warnings indicating the affected zone;

— provide warning in the event of mains or battery failure; and

— alert the fire brigade by a direct link system, manual or automatic.

Emergency exits and escape routes should be clearly indicated.

13.9 Laboratory Facilities

Laboratory facilities for testing that is routinely performed by operations staff may be considered for inclusion with a control center. Alternatively, localized laboratory facilities may be considered for inclusion with operator shelters constructed closer to units.

Design and safety requirements for laboratory facilities are not part of the scope of this document, and the user must consult with organizations or personnel who are experienced in the design features unique to laboratories facilities. However, the designs should incorporate the following basic design concepts.

— There should not be direct access between the laboratory area and the control center.

— Laboratories must have separate HVAC and ventilation systems. Vent hoods and exhaust systems shall be suitable for the tasks being performed.

— Laboratories must have separate monitoring and/or protective systems for flammable, toxic materials or asphyxiants and have suitable fire protection systems.

— The effects of failures, material releases, fire or other events in the laboratory system must be carefully evaluated and the impact upon control center operations fully assessed.

13.10 Equipment and Wiring Layout Considerations

Space should be provided for the following electrical, instrument and control equipment and wiring either in the control center or in a satellite facility:

— process control system equipment;

— instrument/electrical maintenance;

— communications systems (i.e. telephone, IT equipment, radios, etc.);

— electrical and instrument wiring and terminations;

— UPS/electric utilities; and

— battery room.

The process control system equipment should be located in an environment that meets the specifications for the equipment. Sufficient space should be provided for the initial installation, future expansion and wiring systems.

The instrument/electrical maintenance personnel may require space to store spare parts, maintain drawings and related documentation and space to calibrate and maintain equipment, etc.

The communications systems for the control center should be located in an environment that meets the specifications for the equipment. This could include telephone systems, IT equipment, radios, network equipment, mass storage devices, system terminals, and system logging printers.

It is extremely important that sufficient space is provided for electrical and instrument wiring and terminations based upon the control system topology. Consideration should be given during the building design phase to the routing of wiring and/or tubing among the process control equipment, auxiliary equipment, control consoles, and field termination areas. Lack of planning in this area could result in last minute trenches or overhead cable trays being installed, thereby resulting in congestion and poor appearance.

Sufficient space or a separate room should be provided to house the uninterruptible power supplies (UPS) equipment and electric utilities. This would include power supplies required for the control systems, computers, auxiliary equipment, power distribution panels, lighting, and emergency lighting circuits. A separate building may be required for motor control centers and large power handling systems not associated with the control center.

Depending upon the design of the UPS system and the batteries being used, a dedicated battery room may be required. This room may need to be vented to the outside of the control building to readily permit the egress of hydrogen formed in the batteries. A doorway may be needed to the outside of the building from this room. The interior surfaces of the room should be acid spill proof, and acid-proof racks should be used. Refer to NFPA 70 and IEEE 484 for additional information.

14 Remote Instrument Enclosure

Remote instrument enclosures, RIE, are usually located adjacent to or within the process area and contain process control equipment and other instrumentation dedicated to one or more process units. This minimizes the amount of the field wiring required. They are considered unmanned enclosures and have different guidelines than a control center building. See PIP ARS3120, *Predesigned Metal Buildings*, for guidelines relating to these types of enclosures.

14.1 General

Remote instrument enclosures can vary in size and complexity dependent on the size and amount of equipment to be housed. The enclosure could range from the single junction box sized enclosure to a walk-in building. The need for HVAC and purging equipment will depend on the equipment and where the enclosure is located.

14.2 Location

Remote instrument enclosures, where practical, should be installed in non-hazardous locations as defined by NFPA 500 and API 500. If they are located in an electrically classified area, the equipment must meet the classification or the enclosure must be pressurized to make the interior non-hazardous in accordance with NFPA 70 and NFPA 496.

14.3 Construction

The remote instrument enclosure construction is dependent on local requirements and site standards. It may be a standard instrument enclosure (i.e. junction box), custom-built building or a prefabricated self-contained building.

Blast-resistant design should be evaluated for enclosures that contain critical equipment for plant operation or accommodate equipment shared by two or more process units.

14.4 HVAC System

When required, the HVAC system should be designed to maintain conditions suitable for the equipment in the remote instrument enclosure. The cooling and heating capacity of the system should be sufficient to handle all equipment in

the house plus an allowance for future expansion. The need for backup HVAC equipment, louvers, or vents should be considered.

Alarm contacts should be provided to indicate air system failures. All alarm contacts should be relayed back to the main control room and should differentiate between partial and complete loss of air-conditioning or heating.

14.5 Ancillary Equipment

The following ancillary should be considered depending on the design of the remote instrument enclosures and equipment:

— a smoke detector system;

— toxic and combustible gas analyzers for personnel protection;

— oxygen deficiency alarms for enclosures that contain nitrogen or other inerts;

— portable fire extinguishers or a fire-extinguishing system suitable for electrical fires; and

— emergency lights [NEC 700-12(a)].

Control panels may be required for ancillary instrument mounting. Examples are compressors, refrigeration equipment or other special purpose instrumentation. These panels may be mounted in the control center or remote locations. See PIP PCSCP001, *Procurement of Control Panels*.

energy API

2008 Publications Order Form

Effective January 1, 2008.
API Members receive a 30% discount where applicable.
The member discount does not apply to purchases made for the purpose of resale or for incorporation into commercial products, training courses, workshops, or other commercial enterprises.

Available through IHS:
Phone Orders: **1-800-854-7179** (Toll-free in the U.S. and Canada)
303-397-7956 (Local and International)
Fax Orders: **303-397-2740**
Online Orders: **global.ihs.com**

Date: _____ ☐ **API Member** (Check if Yes)

Invoice To (❑ Check here if same as "Ship To")

Name:
Title:
Company:
Department:
Address:
City: State/Province:
Zip/Postal Code: Country:
Telephone:
Fax:
Email:

Ship To (UPS will not deliver to a P.O. Box)

Name:
Title:
Company:
Department:
Address:
City: State/Province:
Zip/Postal Code: Country:
Telephone:
Fax:
Email:

Quantity	Title	SO★	Unit Price	Total
	RP 551, Process Measurement Instrumentation		$117.00	
	RP 552, Transmissions Systems		$101.00	
	RP 553, Refinery Control Valves		$91.00	
	RP 554, Process Control Systems: Part 1-Process Control System Functions and Functional Specification Development		$130.00	
	RP 554, Process Control Systems: Part 3-Project Execution and Process Control System Ownership		$100.00	
	RP 555, Process Analyzers		$136.00	
	RP 556, Fired Heater and Steam Generators		$107.00	
	RP 557, Guide to Advanced Control Systems		$91.00	

❑ Payment Enclosed ❑ P.O. No. (Enclose Copy) _____
❑ Charge My IHS Account No. _____
❑ VISA ❑ MasterCard ❑ American Express
❑ Diners Club ❑ Discover
Credit Card No.:
Print Name (As It Appears on Card):
Expiration Date:
Signature:

Subtotal
Applicable Sales Tax (see below)
Rush Shipping Fee (see below)
Shipping and Handling (see below)
Total (in U.S. Dollars)

★ To be placed on Standing Order for future editions of this publication, place a check mark in the SO column and sign here:

Pricing and availability subject to change without notice.

Mail Orders – Payment by check or money order in U.S. dollars is required except for established accounts. State and local taxes, $10 processing fee, and 5% shipping must be added. Send mail orders to: **API Publications, IHS, 15 Inverness Way East, c/o Retail Sales, Englewood, CO 80112-5776, USA.**

Purchase Orders – Purchase orders are accepted from established accounts. Invoice will include actual freight cost, a $10 processing fee, plus state and local taxes.

Telephone Orders – If ordering by telephone, a $10 processing fee and actual freight costs will be added to the order.

Sales Tax – All U.S. purchases must include applicable state and local sales tax. Customers claiming tax-exempt status must provide IHS with a copy of their exemption certificate.

Shipping (U.S. Orders) – Orders shipped within the U.S. are sent via traceable means. Most orders are shipped the same day. Subscription updates are sent by First-Class Mail. Other options, including next-day service, air service, and fax transmission are available at additional cost. Call 1-800-854-7179 for more information.

Shipping (International Orders) – Standard international shipping is by air express courier service. Subscription updates are sent by World Mail. Normal delivery is 3-4 days from shipping date.

Rush Shipping Fee – Next Day Delivery orders charge is $20 in addition to the carrier charges. Next Day Delivery orders must be placed by 2:00 p.m. MST to ensure overnight delivery.

Returns – All returns must be pre-approved by calling the IHS Customer Service Department at 1-800-624-3974 for information and assistance. There may be a 15% restocking fee. Special order items, electronic documents, and age-dated materials are non-returnable.

THERE'S MORE WHERE THIS CAME FROM.

API provides additional resources and programs to the oil and natural gas industry which are based on API Standards. For more information, contact:

API MONOGRAM® LICENSING PROGRAM
Phone: 202-962-4791
Fax: 202-682-8070
Email: certification@api.org

API QUALITY REGISTRAR (APIQR®)
> ISO 9001 Registration
> ISO/TS 29001 Registration
> ISO 14001 Registration
> API Spec Q1® Registration
Phone: 202-962-4791
Fax: 202-682-8070
Email: certification@api.org

API PERFORATOR DESIGN REGISTRATION PROGRAM
Phone: 202-682-8490
Fax: 202-682-8070
Email: perfdesign@api.org

API TRAINING PROVIDER CERTIFICATION PROGRAM (API TPCP™)
Phone: 202-682-8490
Fax: 202-682-8070
Email: tpcp@api.org

API INDIVIDUAL CERTIFICATION PROGRAMS (ICP®)
Phone: 202-682-8064
Fax: 202-682-8348
Email: icp@api.org

API ENGINE OIL LICENSING AND CERTIFICATION SYSTEM (EOLCS)
Phone: 202-682-8516
Fax: 202-962-4739
Email: eolcs@api.org

API PETROTEAM (TRAINING, EDUCATION AND MEETINGS)
Phone: 202-682-8195
Fax: 202-682-8222
Email: petroteam@api.org

API UNIVERSITY™
Phone: 202-682-8195
Fax: 202-682-8222
Email: training@api.org

Check out the API Publications, Programs, and Services Catalog online at www.api.org.

energy API

1220 L Street, NW
Washington, DC 20005-4070
USA

202.682.8000

Additional copies are available through IHS
Phone Orders: 1-800-854-7179 (Toll-free in the U.S. and Canada)
303-397-7956 (Local and International)
Fax Orders: 303-397-2740
Online Orders: global.ihs.com

Information about API Publications, Programs and Services
is available on the web at www.api.org

Product No. C554201