

Process Control Systems— Process Control System Design

API RECOMMENDED PRACTICE 554, PART 2
SECOND EDITION, AUGUST 2023



American
Petroleum
Institute

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. The use of API publications is voluntary. In some cases, third parties or authorities having jurisdiction may choose to incorporate API standards by reference and may mandate compliance.

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.

Users of this recommended practice (RP) should not rely exclusively on the information contained in this document. Sound business, scientific, engineering, and safety judgment should be used in employing the information contained herein.

API publications may be used by anyone desiring to do so. Every effort has been made by the Institute to ensure 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 used. 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.

API is not undertaking to meet the duties of employers, manufacturers, or suppliers to warn and properly train and equip their employees, and others exposed, concerning health and safety risks and precautions, nor undertaking their obligations to comply with authorities having jurisdiction.

All rights reserved. No part of this work may be reproduced, translated, stored in a retrieval system, or transmitted by any means, electronic, mechanical, photocopying, recording, or otherwise, without prior written permission from the publisher. Contact the Publisher, API Publishing Services, 200 Massachusetts Avenue, NW, Suite 1100, Washington, DC 20001-5571.

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.

The verbal forms used to express the provisions in this document are as follows.

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

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

May: As used in a standard, “may” denotes a course of action permissible within the limits of a standard.

Can: As used in a standard, “can” denotes a statement of possibility or capability.

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, 200 Massachusetts Avenue, NW, Suite 1100, Washington, DC 20001. 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, 200 Massachusetts Avenue, NW, Suite 1100, Washington, DC 20001.

Suggested revisions are invited and should be submitted to the Standards Department, API, 200 Massachusetts Avenue, NW, Suite 1100, Washington, DC 20001, standards@api.org.

Contents

	Page
1 Scope.....	1
1.1 General	1
1.2 Document Organization	1
2 Normative References	4
3 Terms and Definitions	5
4 Control System Topology	10
4.1 General	10
4.2 Physical Location of Control Equipment and Subsystems	11
4.3 System Availability	11
4.4 System Maintainability	11
4.5 Control System Performance Requirements	11
4.6 Lifecycle Costs.....	11
4.7 Security of Control System	11
5 Process Control System Types.....	13
5.1 General	13
5.2 Distributed Control Systems	13
5.3 Programmable Logic Controllers	14
5.4 Single Loop Controllers	14
5.5 Hybrid Process Control Systems	15
5.6 Transitional System Designs	15
5.7 Safety Systems.....	15
6 Process Control System Hardware/Software Design Considerations	16
6.1 General	16
6.2 Overall System Design	16
6.3 Controllers	17
6.4 Operator Interface.....	18
6.5 System Workstations	19
6.6 I/O Modules	19
6.7 Serial Digital Communications.....	22
6.8 Field Networks	24
6.9 Complex Instrumentation.....	24
6.10 Subsystem Interfaces	25
6.11 Redundancy.....	25
6.12 System Capacity/Future Expandability	26
6.13 System Performance	26
6.14 Diagnostics	27
6.15 Maintainability	27
7 Process Control System Software Design Considerations.....	27
7.1 Operating System Considerations	27
7.2 System Programming	28
7.3 Configuration and Programming Devices	29
7.4 Configuration/Programming Considerations.....	29
7.5 Software Security.....	30
7.6 Reports and Logs	32
7.7 Batch/sequence Control	32

Contents

	Page
7.8 Communications	32
7.9 Documentation.....	33
8 Alarm Functions	36
8.1 General	36
8.2 Alarm Types	37
8.3 User-defined Functions.....	37
8.4 Diagnostics	37
8.5 Alarm Sequences	38
8.6 Alarm Display Functions	40
8.7 Dedicated Alarm Systems.....	41
8.8 Alarm Record Functions	42
8.9 Alarm Management Functions	43
8.10 Documentation.....	45
9 Interlocks	45
9.1 General	45
9.2 Types of Interlocks	45
9.3 Sensor Considerations	46
9.4 Shutdown Alarms	46
9.5 Pre-shutdown Alarms	46
9.6 Testing	46
9.7 Documentation.....	46
10 Data Management and Documentation	47
10.1 General	47
10.2 Field Instrumentation	47
10.3 Field Instrument Asset Management Systems	48
10.4 Process Control Systems	48
10.5 Other Specialized Systems.....	48
10.6 Engineering Database Systems	48
10.7 Maintenance Management Systems	49
10.8 Process Data Management Systems	51
10.9 Data Integration	51
11 Instrument Power Systems	52
11.1 General	52
11.2 Process Evaluation	52
11.3 Control System Evaluation	52
11.4 Instrument Power System Design	53
12 Electrical Considerations	56
12.1 Grounding	56
12.2 Electromagnetic Interference	56
12.3 Signal Wiring Systems	56
12.4 Communications	57
13 Control Centers.....	57
13.1 General	57
13.2 Control Center Site Selection	58
13.3 Physical Design Criteria.....	59

Contents

	Page
13.4 Control Center Building Design and Layout.....	59
13.5 Control Center Environmental Controls	60
13.7 Floor Design	61
13.8 Control Center Fire Protection	61
13.9 Laboratory Facilities.....	62
13.10 Equipment and Wiring Layout Considerations.....	62
14 Remote Instrument Enclosure	63
14.1 General	63
14.2 Location	64
14.3 Construction.....	64
14.4 HVAC System	64
14.5 Ancillary Equipment	64
Bibliography.....	65

Figures

1 Refinery Control and Automation Functions	1
2 Control System Topology	12
3 Control System Topology—Open Architecture Hybrid Control System.....	12
4 Process Control System Data.....	47

Tables

1 Process Control Systems Life Cycle Overview.....	3
2 Fieldbus—Device Network Classification	24

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 with 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 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 (PCS) 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. The control systems engineer is challenged to maintain a design that allows communications between the control and the business networks but that also maintains safe and reliable operations.
- Advances in field instrumentation design leading to the general use of smart digital field instrumentation. Further advances in fieldbus 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. The smart devices enable very real, albeit basic, “distributed control” across the various real-time devices within the control domain. The degree of such distributed control shall be considered, if it’s within the corporate policy.
- 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, and instead 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 PCS to external interference and requires additional support to keep the operating systems current and secure. Security and virus protection are major concerns of newer PCSs and must be addressed at both the design and operational phases.
- The integration of the human machine interface and communication networks for the PCS and the safety instrumented system (SIS).
- The addition of “wireless process networks” is bringing new challenges and it is transforming the way the information generated in the field sensors is transmitted and the way the facilities are designed.

The result of all these technical advances is that PCSs 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 PCSs and the business functions of an organization; to select and specify the functions that are necessary for a given application; and to implement those functions in a safe, reliable, cost-effective and maintainable manner.

API 554 consists of three documents to better define the processes required to properly scope, specify, select, install, commission, operate, and maintain PCSs. 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

1.1 General

This recommended practice (RP) addresses the processes required to successfully implement PCSs for oil and gas production, refinery, and petrochemical services. The major topics addressed are listed below.

- *Part 1.* The basic functions that a PCS 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 PCS.

[Figure 1](#) shows the general overall scope of oil and gas production, refinery process control, and the associated automation functions, as well as the portions of which this recommended practice addresses.

The general scope of the material covers general industrial process control topics that are applicable to oil and gas production, refineries, and petrochemical facilities.

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 PCSs. 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.

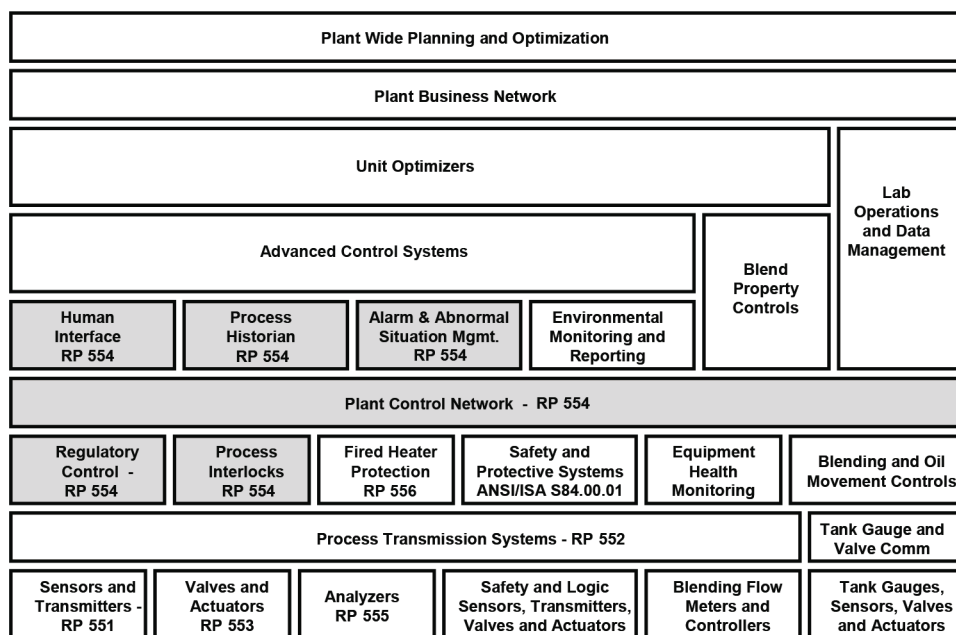


Figure 1—Refinery Control and Automation Functions

1.2 Document Organization

This document is organized to follow the sequence of activities associated with the typical life cycle of a PCS as summarized in [Table 1](#).

The life cycle phases as they apply to PCSs are listed below.

- *Appraise*. Develop business goals and requirements and identify basic functions required. This step is often also referred to as the concept stage.
- *Select*. Further develop business goals and functions into a PCSs scope definition. This step often is part of the early portion of front-end engineering design (FEED).
- *Define*. Finalize PCS's 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, testing, commissioning.
- *Operate*. Commission, operate and maintain.

API 554 consists of three parts, each focusing on a major aspect of PCSs. 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 PCS 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 PCSs 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 PCS.

The portions of API 554 that deal with each phase of the life cycle are identified in [Table 1](#).

Table 1—Process Control Systems Life Cycle Overview

API 554 Section Number	Phase	Objectives	Major Inputs	Major Outputs
Part 1, Sec. 2	Appraise/ concept 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	PCS concept 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, piping and instrumentation diagrams (P&IDs), equipment lists, process hazard analysis — PCS concept design basis	PCS functional specification
Part 2	Define/execute (FEED/ detailed design)	— Prepare request for quote, issue, and select a vendor — Specify hardware, input/output (I/O) layouts, and communications — Design control centers, field devices, interconnecting wiring, instrument power — Define control systems interfaces to other systems and hardware	— PCS 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 factory acceptance 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	— Site acceptance testing of all software-based functions — PCSs ready for operation
Part 3	Operate— commission	Prepare process controls system for operation	Performance requirements	— PCSs in operation — All deficiencies identified and corrected
	Operate— operation	Operate PCS to best operational effectiveness	Performance requirements, consideration of future migrations, upgrades, and managing obsolescence issues	Business revenue and minimal costs
	Operate— maintain	Maintain, preventative maintenance (PM), and repair PCSs	As-built documentation and training	Maximum unit performance and availability

2 Normative References

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any addenda) applies.

API Recommended Practice 552, *Transmission Systems*

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

API Recommended Practice 1167, *Pipeline SCADA Alarm Management*

IEC 61131-3,¹ *Programmable Controllers—Part 3: Programming Languages*

IEC 61158-1, *Industrial Communication Networks—Fieldbus Specifications—Part 1: Overview and Guidance for the IEC 61158 and IEC 61784 Series*

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

IEEE 484,² *Recommended Practice for Installation Design and Installation of Vented Lead-acid Batteries for Stationary Applications*

ISA 18.2,³ *Management of Alarm Systems for the Process Industries*

ANSI/ISA 84.00.01, *Functional Safety: Safety Instrumented Systems for the Process Industry Sector*

ANSI/ISA TR62443-2-3,⁴ *Security for Industrial Automation and Control Systems, Part 2-3: Patch Management in the IACS Environment*

ISO 11064-6,⁵ *Ergonomic Design of Control Centres—Part 6: Environmental Requirement for Control Centres*

NFPA 70,⁶ *National Electric Code*

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

PIP PCCEL001,⁷ *Instrumentation Electrical Requirements*

TIA/EIA RS-232-F,⁸ *Interface Between Data Terminal Equipment and Data Communication Equipment Employing Serial Data Interchange*

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

¹ International Electrotechnical Commission, 3, rue de Varembe, P.O. Box 131, CH-121 Geneva 20, Switzerland, www.iec.ch.

² Institute of Electrical and Electronics Engineers, 1828 L Street, N.W., Suite 1202, Washington, D.C. 20036–5104, www.ieee.org.

³ The International Society of Automation, 67 Alexander Drive, Research Triangle Park, North Carolina 27709, www.isa.org.

⁴ American National Standards Institute, 25 West 43rd Street, New York, New York 10036, www.ansi.org.

⁵ International Organization for Standardization, ISO Central Secretariat, Chemin de Blandonnet 8, CP 401 - 1214 Vernier, Geneva, Switzerland, www.iso.org.

⁶ National Fire Protection Association, 1 Batterymarch Park, Quincy, Massachusetts 02169–947, www.nfpa.org.

⁷ Process Industry Practices, 3925 West Braker Lane (R4500), Austin, Texas 78759, pip.org.

⁸ Electronic Industries Alliance, 2500 Wilson Blvd., Arlington, Virginia 22201, www.eia.org.

3 Terms and Definitions

The following terms and definitions are used in this document. Additional definitions are provided in Parts 1 and 3 when necessary to support the content of those documents.

3.1

batch control

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

A communications network device that allows communications between network branches that use different communications media or protocols.

3.3

business network

A digital communications network that is used for general-purpose business use such as desktop computing, non-process control database applications or other general-purpose applications. Can be referred to as Purdue level 4. Typically, business networks use industry standard communications methods such as Ethernet.

3.4

central control room

CCR

Inhabited facility (typically a building) that houses plant personnel and PCS equipment to permit the operation and coordination of one or more process plants. Control rooms 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.

3.5

continuous control

Control functions that are continuously and repetitively executed to control the values of process variables such as 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.

3.6

control module

A processing module that performs various control and data acquisition functions in a PCS. 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 PCS.

3.7

demilitarized zone

DMZ

A physical or logical subnetwork that contains and exposes an organization's external-facing network services to a larger and untrusted network, i.e. the organization's business LAN or the Internet. The purpose of a DMZ is to add an additional layer of security to an organization's local area network (LAN), by isolating external communications to the process control network.

3.8

discrete control

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.

3.9**distributed control system****DCS**

A general term used for digital PCs 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**electromagnetic interference****EMI**

Electromagnetic interference (may also be known as radio frequency interference [RFI] when applicable to radio frequencies) that may affect an electrical circuit operation due to electromagnetic fields, radiation, or induction, emitted for an external source such as generated by power wiring, motors, or other electrical equipment starting or stopping.

3.11**encryption**

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.

3.12**Ethernet**

Ethernet is an asynchronous communications method that allows messages to collide and 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.

3.13**fieldbus**

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

3.14**field devices**

Any sensors, measuring devices, control elements etc. that are used to sense or directly control process conditions. Current technologies allow increased “intelligence” to be added to the field devices, e.g. self-diagnostics, control functions, and network interconnectivity.

3.15**firewall**

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. See also 3.7, DMZ.

3.16**front-end engineering design****FEED**

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.

3.17**gateway**

A DCS or other PCS module that interfaces communications between foreign devices or devices within the PCS that use differing communications technologies in a structured and secure manner.

3.18**heating, ventilating, and air conditioning****HVAC**

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.

3.19**highway addressable remote transducer****HART**

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. HART™ has evolved to a protocol that enables configuration and messaging of the field device in an effective way. See www.fieldcommgroup.org for more details. HART is an example only, and its inclusion is not intended to endorse it specifically or limit users from considering other applications.

3.20**human machine interface****HMI**

A computing resource for a PCS that is used as an operator's or engineer's interface for displaying data or inputting information or operating commands.

3.21**hybrid control system**

A type of DCS that uses open system technologies to perform PCS functions and that is capable of integrating continuous and discrete control functions within a single control module.

3.22**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.

3.23**Modbus™**

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. Modbus is an example only, and its inclusion is not intended to endorse it specifically or limit users from considering other applications; see www.modbus.org for additional information.

3.24**Object Linking and Embedding****OLE™**

A Microsoft™ standard, object linking and embedding, which defines methods for applications to share common data and applications. OLE and Microsoft are used as examples only, and their inclusion is not intended to endorse them specifically or limit users from considering other applications.

3.25**Open Platform Communications****OPC®**

OPC is the interoperability standard for the secure and reliable exchange of data in the industrial automation space and in other industries. It defines methods for the secure and reliable exchange of data using extensions of OLE standards between multiple vendors (OLE is used as an example only, and its inclusion is not intended to endorse it specifically or limit users from considering other applications). OPC standards provide a common practice for manufacturers of PCSs to make real-time and historical data available to other devices in a structured

and deterministic way. OPC unified architecture (UA) is much more complex than previous OPC specifications and is designed to:

- use cross-platform-capable communication instead of Windows Distributed Component Object Model (DCOM)[™] (Windows DCOM is an example only, and its inclusion is not intended to endorse it specifically or limit users from considering other applications.);
- combine the OPC DA, A&E, HDA functionality into a single set of services (OPC is an example only, and its inclusion is not intended to endorse it specifically or limit users from considering other applications.);
- model complex data structures for collaboration with other standards organizations;
- be implementable on different platforms, from embedded systems to enterprise systems.

See <http://www.opcfoundation.org> for additional information.

3.26

open systems

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.

3.27

operability

The characteristics of a PCS 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.

3.28

personal computer

PC

A computing resource that has multiple uses. It is intended for use by a single user and may have several noncontrol applications installed.

3.29

process control module

Some type of computing resource, either of proprietary design or a commercially available computer that performs process control-related functions including data acquisition and control functions.

3.30

process control network

PCN

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.

3.31

process control system or basic process control system

PCS or BPCS

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. SIS functions are considered to be separated from the PCS functions but can share communication network components, engineering tools, and HMI.

3.32**process hazard analysis****PHA**

A hazard analysis technique for process plants.

3.33**process interlocks**

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.

3.34**process safety management****PSM**

A management process that results in process hazards being identified and suitable safeguards established, and that provides management of change procedures that ensure that changes to processes are similarly addressed.

3.35**programmable logic controller****PLC**

A stand-alone or separately networked microprocessor-based control module that performs a variety of data acquisition and control functions. Most functions performed are discrete control functions, but continuous functions may also be performed. A PLC typically will have its own dedicated I/O equipment and may also have dedicated shared display functions.

3.36**radio frequency interference****RFI**

Electromagnetic 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. See also EMI definition in 3.10.

3.37**relational databases**

Relational databases use tables to store location information, and the data are accessible by fields, allowing access to locate specific answers to generated queries in a short time duration.

3.38**reliability**

The probability that a system or device will perform its function when required.

3.39**remote instrument enclosure or remote input outputs****RIE or RIO**

An unmanned facility that houses process control systems equipment and other support equipment required for control and monitoring of a process plant or plants. RIEs/RIOs may be built-in-place structures, prefabricated structures, or simple self-contained junction box type enclosures.

3.40**router**

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

3.41**safety instrumented system****SIS**

A system that is intended to protect against specific identified process hazards.

NOTE SISs are not within the scope of this RP. For further details refer to ANSI/ISA 84.00.01

3.42

safety integrity level

SIL

The availability required for the SIS. SIL is a measure of the probability that the SIS will operate when required to.

3.43

safety module

A control module that is specifically designed to meet the functional and security requirements for use with safety instrumented systems, which may be integrated within the overall PCS design.

3.44

sequencing control

Control functions that involve a series of steps, usually involving discrete controls, that are executed in a predefined order and that may include conditional steps, branching and loops. Normally, sequencing control is a portion of a larger processing scheme and does not produce a final or intermediate product.

3.45

switch

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.

3.46

workstation

A computing resource that is used for general business functions such as e-mail, word processing, internet access, etc. but not used as a PCS HMI.

4 Control System Topology

4.1 General

Control system topology is the general layout of the PCS describing interconnections between major components. The system topology should be based primarily on the functionality and security of the control equipment, communications and subsystems, 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 PCS.

The PCS topology should be developed with consideration of the functions identified as the practices discussed in API Recommended Practice 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 subsystems together.

[Figure 2](#) and [Figure 3](#) show two examples of topology. These are presented as illustrations; other designs exist too. [Figure 2](#) represents a typical proprietary distributed control system found in many plants. This system is characterized by at 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 hardwired I/O.

[Figure 3](#) illustrates a modern open architecture system that 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 need to be addressed are discussed in the following sections.

4.2 Physical Location of Control Equipment and Subsystems

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 to 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.

4.3 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 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.

4.4 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 to facilitate this process. Additional control module redundancy may be necessary to meet system maintainability.

The characteristics of the process being controlled shall also be considered when evaluating 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 process areas that cannot or do not come down together do not share key equipment.

4.5 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.

4.6 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 shall be considered and often provide justification for more robust and secure designs.

4.7 Security of Control System

Security considerations that affect the topology of the control system include firewalls, DMZs, communications servers, communication encryption (including wireless), and restricted data links. Several older generation systems also employ proprietary communications; however, not all systems are open systems. Most of these issues shall be identified and addressed during the PCS functional specification development process described in API 554, Part 1. Also, See ANSI/ISA 99.00.01 for comprehensive discussions of PCS security issues and resources. A detailed discussion of PCS security is a complex and extensive issue and is beyond the scope of this document, although some basic considerations are described in [7.1](#).

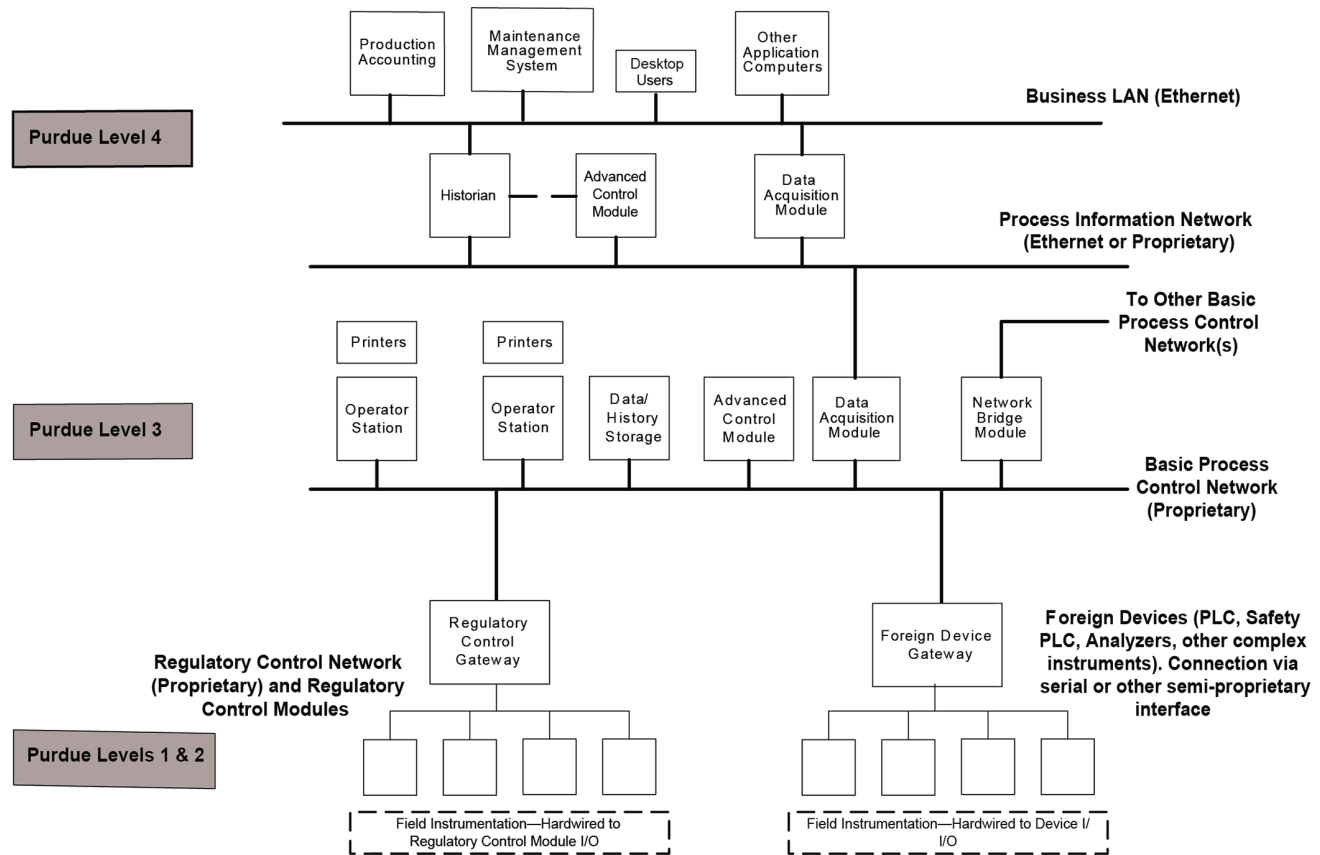


Figure 2—Control System Topology

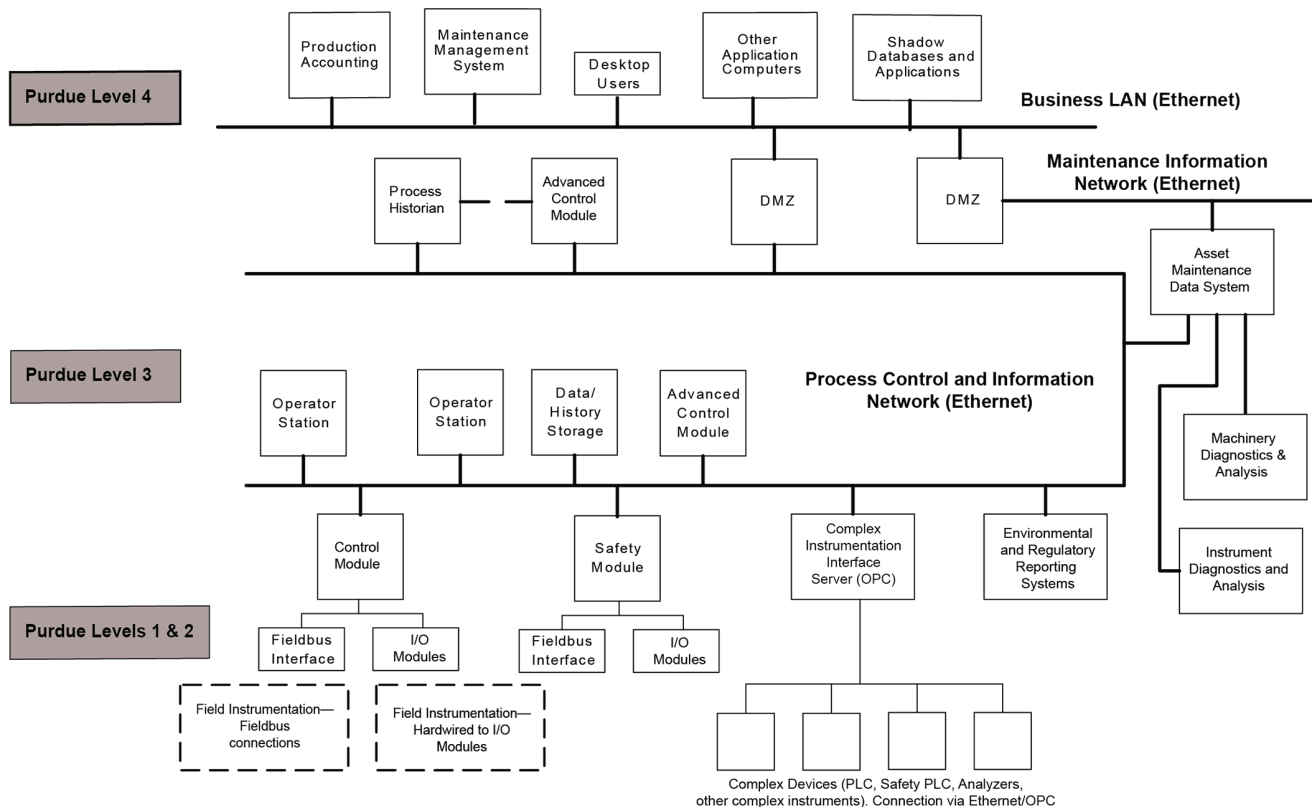


Figure 3—Control System Topology—Open Architecture Hybrid Control System

5 Process Control System Types

5.1 General

There are several types of systems that may be used a part of a PCS. The selection of hardware and software implemented in a specific PCS 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 shall define the functions that will be implemented and what types of architecture, communications, and hardware will be used.

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

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

5.2 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 configuration 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. Generally DCS employ a single database, which means modifications to the configuration are only required to take place in one location, and other functionality employed in the system that uses this database will automatically be revised to the single change.

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, I/O modules, processors, and other power and communications support for the module to function. The control strategies are configured, and there are many standard, special, and optional functions available. Normally, the systems programming and configuration 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. Configuration of these systems is normally undertaken from a single tool, which provides for control strategy, historization requirements, alarm and event recording, trending, security access to the data, or changing the parameters of the data, etc.

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. Typically this has been a proprietary closed design provided by the DCS manufacturer; however, current systems are deployed using a more open network approach.

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

Gateway modules to provide a variety of interfaces to third-party subsystems or computer systems. These are usually proprietary design modules that interface to open systems communications such as Ethernet, Modbus, or other technologies. Modbus is an example only, and its inclusion is not intended to endorse it specifically or limit users from considering other applications.

5.3 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. 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 previous experience interfacing with a hybrid control system vendor. PLC vendor should provide certified hardware and software interfaces. A much more typical implementation is through interface servers that use standard methods, such as OPC (OPC is an example only, and its inclusion is not intended to endorse it specifically or limit users from considering other applications).

PLCs may be applied in several roles and are often used in specialty applications provided by third parties. The PCS functional requirements should be considered when applying PLCs. While designs vary, PLC applications are typically less robust than integrated PCSs (DCS or hybrid systems) and are often more complex to implement in larger systems. This is due in part to the fact that PLCs have tended to operate with a multiple database concept as opposed to a single relational database used in DCS systems. Current developments have caused some PLC system providers to move towards the single relational database environment for their individual equipment.

Some of the applications for PLCs are as follows.

- A stand-alone PLC that is capable of performing control functions associated with several smaller applications within a process area, or one large function such as sequence control, particularly when a third party is supplying a package subsystem (i.e. manufactured skid for a particular purpose).
- A PLC that is designed as an integral part of a general-purpose PCS that performs most of the functions required in the PCSs.
- 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 configuration. 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.

5.4 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.