Process Control Systems

Part 1—Process Control Systems Functions and Functional Specification Development

API RECOMMENDED PRACTICE 554
~~SECOND~~ THIRD EDITION, ~~JULY 2007~~DRAFT

Process Control Systems

Part 1—Process Control Systems Functions and Functional Specification Development

Downstream Segment

API RECOMMENDED PRACTICE 554
~~SECOND~~ THIRD EDITION, ~~JULY 2007~~DRAFT

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 following definitions apply:

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Generally, API standards are reviewed and revised, reaffirmed, or withdrawn at least every five years.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 and updated quarterly by API, 1220 L Street, N.W., Washington, D.C. 20005.

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

Figures

Tables

Process Control Systems
Part 1—Process Control Systems Functions and Functional Specification Development

1 Overview

1.1 INTRODUCTION

Advances in computing and digital communications technologies since the preparation of the 1st edition of API RP 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~~shall be approached and have created major issues relative to system design and system security. These issues are:

- 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 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 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.
- 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.
- The integration of the Human Machine Interface and communication networks for the Process Control System (PCS) and the Safety Instrumented System (SIS).
- The addition of "process wireless 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.
- Security and virus-protection are major concerns of newer Process Control Systems and ~~must~~shall 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.

The API 554 consists of 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.

1.2 SCOPE

This Recommended Practice addresses the processes required to successfully implement Process Control Systems for oil & gas production, refinery and petrochemical services. The major topics addressed are:

- 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.

- Practices to select and design the installation for hardware and software required to meet the functional and integration requirements.

- 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 oil & gas and refinery 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 & 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 recommended practice 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.

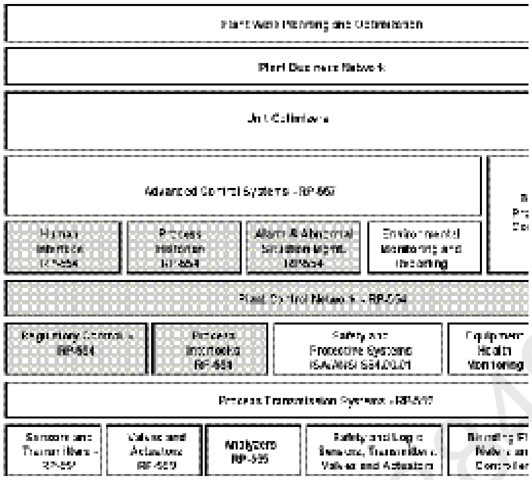
Plant Wide Planning and Optimization
Plant Business Network
Unit Optimizers
Advanced Control Systems – RP 557
Human Interface RP 554
Process Historian RP 554
Alarm & Abnormal Situation Mgmt. RP 554
Environmental Monitoring and Reporting
Plant Control Network – RP 554
Regulatory Controls – RP 554
Process Interlocks RP 554
Safety and Protective Systems ISA/ANSI S84.00.01
Equipment Health Monitoring
Process Transmission Systems – RP 552
Sensors and Transmitters – RP 551
Valves and Actuators RP 553
Analyzers RP 555
Safety and Logic Sensors, Transmitters, Valves and Actuators
Blending Fl Meters an Controller

Figure 1—Refinery Control and Automation Functions

Comment [PGJH1]: Improve graphic quality. Graphic source is needed. Action by API Editor

1.3 DOCUMENT ORGANIZATION

This document is organized to follow the sequence of activities associated with the typical lifecycle of a Process Control System as summarized in Table 1.

The lifecycle phases as they apply to Process Control Systems are:

- 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, and specifications and procure other hardware and equipment. This step often forms the bulk of Front End Engineering Design (FEED).

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

- Operate—Commission, operate and maintain.

Table 1—Process Control Systems Lifecycle Overview

RP 554 Section Number	Phase	Objectives	Major Inputs	Major Outputs

Part 1, Section 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, Sections 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 Systems 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

API RP 554 consists of three parts, each focusing on a major aspect of Process Control Systems. The three parts and the areas that they cover are:

- 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 Systems.

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

1.4 REFERENCED PUBLICATIONS

A number of publications are either directly referenced in the discussions in Parts 1, 2 and 3 of API RP 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

RP 551	*Process Measurement Instrumentation*
RP 552	*Transmission Systems*
RP 553	*Refinery Control Valves*
RP 555	~~555~~ *Process Analyzers*
RP 556	*Instrumentation, Control, and Protective Systems for Gas Fired Heaters*
RP 557	*Guide to Advanced Control Systems*
RP 750	*Management of Process Hazards*

~~AIChE[1]~~

~~*Guidelines for the Safe Operation of Chemical Processes*~~

~~*Layer of Protection Analysis: Simplified Process Risk Assessment*~~

EEMUA[2]

191	*Alarm Systems—A Guide to Design, Management and Procurement*
201	*Process Plant Control Desks Utilizing Human-Computer Interfaces A Guide to Design, Operational and Human Interface Issues*

~~[1] American Institute of Chemical Engineers, Center for Chemical Process Safety, 3 Park Ave, 19th floor, New York, New York 10016-5991, www.aiche.org/ccps.~~

[2] The Engineering Equipment and Materials Users' Association, 10-12 Lorat Lane, London, EC3R 8DN, United Kingdom, www.eemua.org.

IEC[3]

61131 *Programmable controllers, Part 3, Programming languages*

61508 *Functional safety of electrical/electronic/programmable electronic safety related systems, Parts 1 – 7*

61511 *Functional safety instrumented systems for the process industry sector, Parts 1 – 3*

~~61158~~ ~~*Digital data communications for measurement and control—Fieldbus for use in industrial control systems, Parts 1 – 7*~~

61512 *Batch control—Parts 1 – 3*

62951~~*, WirelessHART – [????]*~~Industrial Communicating Networks Wireless Communication. Network and Communication Profiles – Wireless Hart

ISA[4]

S18.1 *Annunciator Sequence and Specifications*

84.00.01 (IEC 61511 Mod) *Application of Safety Instrumented Systems for the Process Industries*

S88.01 *Batch Control Systems: Models and Terms*

~~S91.00.01~~ ~~*Identification of Emergency Shutdown Systems and Controls That Are Critical to Maintaining Safety in Process Industries*~~

S95.01 *Enterprise-Control System Integration—Part 1: Models and Terminology*

100 ~~[**Wireless ????**]~~*IEC 62734 Industrial Communication Networks – Fieldbus Specifications – Wireless Systems for Industrial Automation: Process Control and Related Applications*

OSHA[5]

29 *CFR* 1910 *Code of Federal Regulations Title 29—Occupational Safety and Health Standards*

PIP[6]

PCESS001 *Safety Instrumented Systems Guidelines*

~~PCED001~~ ~~*Guide for Control System Documentation*~~

1.5 DEFINITIONS

The following terms and definitions are used in this document. Additional definitions are provided in Parts 2 and 3 when necessary to support the content of those documents.

[3] International Electrotechnical Commission, 3, rue de Varembe, P.O Box 131, CH-1211 Geneva 20, Switzerland, www.iec.ch.

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

[5] Occupational Safety and Health Administration, U. S. Department of Labor, 200 Constitution Avenue, NW, Washington, D. C. 20210, www.osha.gov; *The Code of Federal Regulations* is available from the U. S. Government Printing Office, Washington D. C. 20402.

[6] Process Industry Practices, 3925 West Braker Lane (R4500), Austin, Texas 78759, www.pip.org.

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.

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.

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

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.

~~**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 Recommended Practice, a DMZ is located between a business LAN and the process control network.~~

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.

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.

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.

Ethernet: Refers to a networking standard that uses a single cable consisting of 4 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 802.x series of standards.

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.

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 fieldbus 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.

Field Devices: Refers to any sensors, measuring devices, control elements etc. that are used to sense or directly control process conditions.

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.

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.

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.

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 – 20 m~~a~~A analog signals. See www.hartcomm.org for more details.

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.

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.

~~**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.~~

Object Linking and Embedding (OLE): Refers to a Microsoft standard, which defines methods for applications to share common data and applications.

OLE for Process Control (OPC): Refers to a series of standards 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.

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.

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.

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.

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.

Process Control System~~s~~ or Basic Process Control System (PCS or BPCS) : 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 a process unit or area. Safety instrumented systems functions are considered to be separated from the process control system functions but can share communication network components, engineering tools and HMI

~~**Process Hazard Analysis (PHA):** A hazard analysis technique for process plants.~~

~~**Process Interlocks:** Refers to discrete control functions that cause automatic actions to occur but which are not specifically designated as being safety related.~~

Process Safety Management (PSM): 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.

Programmable Logic Controller (PLC): Refers to 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.

Redundant Array 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.

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

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.

~~**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 Recommended Practice.~~

~~**Safety Integrity Level (SIL):** Refers to the availability required for a Safety Instrumented System (SIS). SIL is a measure of the probability that the SIS will operate when required to.~~

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.

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.

Virtual Private Network (VPN): The use of encryption to implement a 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.

Wide Area Network (WAN): A communications network that uses such devices as common dedicated communication systems to span a larger geographic area than can be covered by a LAN.

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.

2 Process Control System Planning and Conceptual Design Basis

This section describes the process required to develop the overall requirements for a Process Control System prior to starting detailed design. Changes in control and information system technology have allowed the Process Control System to perform many more functions and interface with other business activities. In some cases, the Process Control System may perform some business functions that were not historically possible to do within previous technologies. Therefore, it is critical to define the boundaries of the Process Control System and the functions to be performed. The results of this process will have substantial impact upon initial implementation cost, schedule, lifecycle cost, operability and maintainability of the Process Control System, especially if needed functions are not identified prior to design.

2.1 BUSINESS DRIVERS

The design of a Process Control System is ultimately determined by business needs and economic justifications of each of its functions. Many functions are required just from an operating necessity point of view—a Process Control System is required to operate a process. Some of the other business related functions performed by a Process Control Systems will be determined by other business needs.

The topics addressed in this section identify many of the business related requirements that a Process Control System may have to address. However, these functions should be justified against a specific business need. The economic drivers for a Process Control System vary widely with the business requirements. Some of the more common economic issues are:

- Safety of the overall plant operation.
- Accuracy and repeatability of Process Control System operation and dynamic performance.
- Maintenance costs, spare parts availability and support availability.
- Reliability of the Process Control System and its impacts upon process availability.
- Flexibility to allow expansion, modification and improvements.
- Functions to support business demands such as data collection and reporting, computing of key performance indicators and similar functions.
- Operation efficiency through improved operator and maintenance interfaces.
- Strategic business issues associated with development and support of new and developing process control, measurement and communications technologies.

2.2 PROCESS CONTROL SYSTEM CONCEPTUAL DESIGN BASIS

Prior to the start of detailed engineering, a conceptual design of the Process Control System should be clearly documented in a Process Control System conceptual design basis that is reviewed and approved.

This process requires a working knowledge of the content of this recommended practice and an understanding of company business philosophy and the specific project business objectives. In addition, any management guidelines or existing company standards, practices, procedures, infrastructure, etc. should be identified as applicable or not.

A fundamental issue with definition of the conceptual design of a Process Control System is to define the functions that the system ~~must~~shall provide and how it interacts with other systems and functions, either existing or planned. This conceptual design definition will identify the Process Control System boundaries.

2.3 INPUT REQUIREMENTS

Development of the conceptual design basis for a Process Control System requires inputs from a number of different functional areas. These are listed below and discussed in more detail in the following sections.

- Corporate standards and practices.
- Operations.
- Maintenance.

- Engineering.
- Business planning and scheduling.
- Environmental.
- Process safety management.
- Information technology.

2.3.1 Corporate Standards and Practices

Corporate or local standards and practices may dictate what Process Control System alternatives make economic and practical sense for a particular application. While existing standards and practices can be a very helpful guide in assessing the scope of a Process Control System, careful consideration ~~must~~shall also be given to advances in process control technology since the standards and practices were established.

The questions listed below should be considered during development of Process Control System scope. As the analysis progresses, other related local issues may also be applicable.

2.3.1.1 Is there a facility master plan for automation that determines the basic system architecture and the support functions that are available or to be supplied? Is there an overall migration plan for adoption of new technologies?

2.3.1.2 What are the applicable existing plant or corporate standards or procedures that apply? Does the new control system design have to match existing installations? Does the projected useful life of existing installations justify continuing with the technology, or is a general upgrade of technology justified by business needs? Are there other existing installation or infrastructure issues that ~~must~~shall be considered?

2.3.1.3 Are there predefined “Best Practices” for subsystems or applications within the overall project?

2.3.1.4 What other support functions are required of the Process Control System that ~~must~~shall be accommodated in the basic control system design?

2.3.1.5 What are the facility and company requirements relative to sharing of data, data validation, data security, and other related issues? Since the Process Control System ~~must~~shall be very secure from unauthorized changes, the methods by which these various functions communicate with the process operator and with each other is a critical portion of the Process Control System design.

2.3.1.6 What are the corporate process control network security standards? What protection layers are required to segregate the process control network from outside systems?

2.3.1.7 What physical security practices are to be followed such as card access to control rooms or equipment rooms, video surveillance, etc.?

2.3.2 Operations

Operations organization, practice, procedures and staffing have considerable input to Process Control System functional requirements. The following questions should be evaluated in assessing operational considerations for a Process Control System. These questions are presented in three broad areas:

- Operational issues dealing with how a plant is to be operated and staffed.
- Physical issues associated with physical layout, space requirements and provisions for future expansion.
- Interface issues with other applications, business systems and devices that are not integral with the Process Control System.

2.3.2.1 Operational Issues

- How are process unit operations divided among operators? What are the risk areas? Should each risk area be controlled by a set of HMI, controller and subsystems? How many HMIs are required per unit? Is backup coverage of unit operations required among HMIs?

- How are operating procedures for normal and abnormal situations documented and accessed? Is it desirable to automate certain procedures, due to complexity or other considerations?

- How many console operators are required? How many control loops is each operator expected to handle?

- Where are outside operators located and how do they interact with the console operator(s)? What functions will they perform? What level of local control, monitoring and operation is required and are there any constraints on how such local control is achieved? What is the minimum staff required to deal with emergency situations?

- How are outside battery limits and utility systems operated? What requirements are there to view sections of a plant that are not controlled by that HMI?

- Does the process involve batch operations that need to make use of ISA 88.01 batch control functions and practices?

- What is the interval between planned unit turnarounds? Is the Process Control System shared among units that are not scheduled for turnarounds at the same time?

- What types of remote operations will be required vs. local monitoring and operator actions? Are there remote facilities to be controlled by this control system? If so, what are the design parameters for such remote control, including security?

- How are alarms communicated to the operator? What are all the sources of hard and soft alarms? What provisions are required for alarm management and screening and analysis? Is a separate alarm system required?

- How is the process operator to enter and monitor the status of work orders? How is the process operator to respond to system maintenance alarms?

- Will a process operator training system be installed? What fidelity will be required for the process model? Will the model be required to run faster than real time? Will the training system be required to upload the current operating system configuration and status or a snapshot of the unit operation as a starting condition? If the training system is to be identical to the operating system, how will the two be isolated such that training actions do not affect current operations? Is the training system to be used for engineering analysis and design "what-ifs?"

2.3.2.2 Physical Issues

- Where are HMIs going to be located? Is there a central control room? Where is it relative to the plant? Will the building that houses the HMI serve as or be considered an emergency gathering area? Will any of the HMIs be located in electrically classified areas, and if so, what classifications ~~must~~shall be met?

- How many and what type of HMI stations are required? Are remote interface stations required? Are there any special operator interface requirements such as portable interfaces, handheld view and data entry functions, etc.?

- What space requirements are required to accommodate workstations needed for access to business functions such as e-mail and word processing?

- Will lifecycle requirements for the installation require provisions for expansion or upgrade over its life; is this a complex wide system or single plant/unit? What is the required service life?

- What provisions need to be made for expansion? Is spare capacity or room to expand required?

- Are there specific drawing standards for process graphics, such as: specific symbol usage and interpretation, line weights, line color codes, overall graphics layout, density, etc.?

- Are third party vendors permitted to access data from specific devices, such as turbines and compressors to provide monitoring and diagnostic assistance? If so, what are the specific security and other procedures?

2.3.2.3 Interface Issues

- What functions associated with plant security will operators be responsible for monitoring—should the operators console incorporate video capability?

- Are special purpose operator interfaces required for specialty control systems such as compressor or turbine controls, stand alone PLC, analyzers, etc.? If so, where are these located? What information ~~must~~shall be displayed on the HMIs? How are the systems connected to the HMIs? What are the security provisions required?

- What interfaces are required to other specialty systems that may have local PLC or other types of controls? What information ~~must~~shall be displayed at the HMIs? What are the security provisions?

- What level of redundancy, security, availability and reliability is required? Are process shutdowns due to control system failure acceptable or ~~must~~shall the design be robust enough to tolerate failures? What provisions are required to allow manual operation or override of automatic operation?

- Is there a need to consider demands upon the control system for functions that may not be typically considered by design engineers? Examples are environmental reporting, alarm filtering, sequence of events, computations, etc.

- What communications requirements exist? Do operators have radios or other communications with control centers?

- Are there requirements for video monitoring of flares, process areas or other video applications? Are these to be incorporated into the Process Control System?

- How does the operator interface with laboratory systems? How are samples labeled and how does the operator obtain laboratory results?

- Are on-line documentation and help systems to be available within the Process Control System or only from the Business LAN? Will the process operator have the ability to make entries into the help system for future reference?

- If documents are to be available within the Process Control System, will the Document Management System entries be coded such that the right document can be displayed within the Process Control System within the context needed? For example do help documents or procedures need to be tied to specific graphics or alarms? If such access is permitted does this require the documents to reside on the control LAN? If not, then how is the Process Control System security and integrity assured?

2.3.3 Maintenance

The maintenance functions include all the activities required to monitor, evaluate, repair or enhance equipment health, suitability for service, or run time on the equipment that are part of, or accessed through the Process Control System.

2.3.3.1 What requirements are there to match existing instrumentation and Process Control System equipment and systems to minimize maintenance spare parts inventory costs, training costs, and maximize maintenance effectiveness?

2.3.3.2 What requirements are there for on-stream monitoring, diagnostics and communication with field instrumentation? Is this system required to be part of the Process Control System? If not, ~~must~~shall it be interfaced with the Process Control System? How are diagnostics historized and communicated to operations and maintenance personnel? Are maintenance work practices able to make use of the information? What is the data access interval for such data?

2.3.3.3 What other instrument systems such as vibration monitoring systems that are used for maintenance diagnostics and equipment health monitoring are required? How is the information communicated to the end users? Does the information pass through the Process Control System? Is it monitored by the process operators? For instance, ~~must~~shall a turbine event log be captured such that the last x minutes can be transferred to the maintenance personnel to analyze the failure?

2.3.3.4 Are work requests and orders and other maintenance activities handled through the Process Control System? Is the Process Control System maintenance handled through the corporate ERP maintenance system?

2.3.3.5 What level of on-stream Process Control System modifications or maintenance may be required and how can these modifications be made? This applies to both software upgrades and hardware repairs, additions or upgrades.

2.3.3.6 What maintenance activities, such as field instrument configuration, will need to be performed through the Process Control System? Is a separate interface station required? What security features ~~must~~shall be in place to prevent unauthorized modifications?

2.3.3.7 If more than one operating unit is controlled through a single Process Control System, how will maintenance on one of the units be accomplished if some of the units are still operating? What portion of the configuration can be changed when the system is on-line and what parameters require the Process Control System to be taken off-line and for how long? Is there ever a period of time where all units on a single Process Control System will be shut down to allow for system wide maintenance that cannot be performed while a unit is operating?

2.3.4 Engineering

Engineering refers to engineering activities required to perform initial configuration and programming activities and to support a business after the Process Control System is installed and commissioned.

2.3.4.1 What data ~~must~~shall be captured for purposes of process evaluation? How much history ~~must~~shall be retained, what is the required fidelity, is data compression allowed, how is it viewed, and how many years of data ~~must~~shall be available on-line?

2.3.4.2 What tools ~~must~~shall be available to maintain Process Control System configuration and programming? Is a separate engineering station or application required? What security requirements ~~must~~shall be available to assure system integrity and audit trails?

2.3.4.3 Is there a mechanism to perform initial population of the configuration data from an engineering database? Will this mechanism be a one-time transfer or will it be required for ongoing transfers of new engineering data? How is the accuracy of bulk transfers assured?

2.3.4.4 What tools are required to monitor Process Control System performance and effectiveness?

2.3.4.5 What requirements are there to interface the basic control system with advanced control systems? What additional hardware, software and interfaces are required? (See API RP 557 for additional information.)

2.3.4.6 What requirements exist for the Process Control System to communicate with other plant wide control systems?

2.3.4.7 What requirements are there for an engineering development system to be used during design engineering? Will this system be used later for training or a source of spare parts?

2.3.4.8 What requirements are there for engineering to develop or identify and document configuration, graphics and other engineering standards?

2.3.4.9 What requirements are there to segregate control functions in different hardware, or to segregate control from Safety Instrumented Systems (SIS)?

2.3.4.10 What are the system performance criteria such as controller execution rate, maximum acceptable loading, spare I/O, processing and communication capacity, expandability and network loading. What performance criteria are required to meet the reliability and availability goals?

2.3.5 Business Planning and Scheduling

The business planning and scheduling functions include all the procedures, methods, tools and techniques to be performed within the Process Control System to facilitate business planning and scheduling or to provide the data for such activities.

2.3.5.1 Is compliance with ISA 95.01 *Enterprise-Control System Integration* or ISA S88.01 *Batch Control Systems* required?

2.3.5.2 What process data needs to be transferred to yield accounting and production record systems? Is the data obtained from a historian, or via direct access? What is the fidelity of that data? What compensations are required for stream properties?

2.3.5.3 What functions are required to monitor and predict inventory and quality of raw materials, finished products, intermediates and by-products?

2.3.5.4 How are production plans communicated to unit operations? How are inventory control plans and results communicated?

2.3.5.5 How are production plans communicated to raw material procurement and final product shipping and handling?

2.3.5.6 How is lab data communicated to planning and scheduling functions? How is this data evaluated?

2.3.6 Environmental

The environmental functions include all the operational constraints, rules, procedures, methods, tools and techniques to be performed within the Process Control System to facilitate environmental compliance or to provide the data for such activities.

Environmental monitoring and reporting requirements are usually dictated by regulatory authorities and may have a major impact upon the Process Control Systems functions and the overall cost and performance of the system, especially if these considerations are not included in the Process Control System design basis and have to be added at a later date.

2.3.6.1 What environmental information ~~must~~shall be captured? How is this information to be captured? What are the rules for incomplete or missing data? What are data validation and audit trail requirements for environmental data? Are these rules to be applied within the control system?

2.3.6.2 What are the requirements to record and report environmental performance? Are these records internal to the Process Control System, to the company, or ~~must~~shall they be reported to one or more regulatory agencies directly from the Process Control System? If so, how?

2.3.6.3 How is environmental performance monitored by operations? How is operations made aware of potential violations or approaches to potential violation? How is the Process Control System to mitigate potential violations?

2.3.7 Process Safety Management

The Process Safety Management (PSM) functions include all the operational constraints, rules, procedures, methods, tools and techniques to be performed within the Process Control System to facilitate PSM compliance. The basic requirements for PSM are stated in OSHA 1910.119 and API RP 750.

2.3.7.1 How is the overall safety of the process and its Process Control System going to be evaluated?

2.3.7.2 Will Safety Instrumented Systems (SIS) exist for this process? If so, ANSI/ISA 84.00.01 (IEC 61511 Mod) and associated rules also apply to those portions of the system. Will the Process Control System act as the HMI for the SIS to monitor, historize and annunciate SIS related status and alarms? Will the interface be a digital or hard-wired interface?

2.3.7.3 What is the role and what are the requirements of the Process Control System in facilitating PSM Compliance?

2.3.7.4 What are the management of change processes and required records? What procedures exist to ensure that changes to data that appear in several systems are coordinated?

2.3.7.5 What requirements exist for protection of operating personnel from process hazards? Are blast resistant buildings or remote control centers required?

2.3.7.6 What level of training and refresher training is required? Is a process simulator required? How are operations and maintenance personnel qualified to interact with the Process Control System? How is it ensured that a simulator cannot interact with the actual process?

2.3.7.7 What alarm management functions are required to avoid a proliferation of alarms that could degrade the process operator's performance, particularly in a crisis situation?

2.3.7.8 What alarm management functions are required to handle start-up, shutdown or alternative operating cases? Are dynamic set points or alarm priorities required to handle these cases?

2.3.8 Information Technology

Information technology functions include all the procedures, methods, tools and techniques necessary to facilitate the exchange of information between the Process Control System and business applications. Within the context of defining Process Control Systems requirements, the IT function is usually to provide the tools and mechanisms and security requirements for transfer and use of Process Control System data and not to define the applications themselves. The answers to the following questions should be developed from a collaborative effort of all of the groups described in this section working with IT, and should identify both data read from the Process Control System and data that is transferred from business applications to the Process Control System.

2.3.8.1 What business applications exist, or which ~~must~~shall be created, that need to receive data from, or send data to the Process Control System? Examples of these applications are yield accounting, planning and scheduling, laboratory systems, environmental reporting, business side historians and similar applications.

2.3.8.2 What other applications are there that directly interface between the Process Control System and the business LAN? Examples of these types of applications are historians, process and equipment diagnostic and analysis programs, documentation programs, alarm management programs, etc.?

2.3.8.3 What data ~~must~~shall be transferred between this Process Control System and systems residing on the business LAN? What are the types of data, quantity, quality and frequency required of data transfers?

2.3.8.4 How is data to be transferred between systems? Are the methods (protocols, message structures, etc.) for systems outside this control system to communicate with the Process Control System defined? Are these proprietary techniques or industry standards based, such as XML? Do the methods vary by system? Are the methods different for transfers that go outside the control system LAN to the Business LAN or to third party systems inside or outside the physical boundaries of the plant?

2.3.8.5 What security requirements are necessary to prevent malicious virus or other software from affecting Process Control System performance, reliability and safety? Will a DMZ or shadow databases be required to prevent propagation or unauthorized access to the Process Control System?

2.3.8.6 How is the process data historian going to be used? What applications will require data from the historian or will write data to the historian? Is the historian used as the buffer between business applications and the Process Control System? Where in the system does the historian reside? On the Process Control System? On the business LAN?

2.3.8.7 What levels of data validation, and confidence level are required? Does data confidence level need to be tracked real-time? If so, what are the rules and which specific points are involved?

2.3.8.8 Is there a requirement for process and environmental data to pass from the Process Control System through the information system or process historian to external systems or pass directly to external regulatory bodies from this control system? Are parallel data paths, shadow servers, RAID drives etc. required to prevent missing data during system failures or maintenance?

2.3.8.9 What are the explicit security measures required to protect the integrity of the Process Control System, given that the control LAN and/or the business LAN is likely to be interconnected with the outside world in one or more ways? ~~Must~~Shall downloaded data be reviewed; modified, if necessary; and accepted by the process operator? ~~Must~~Shall any changes be audit trailed?

2.3.8.10 How is open data access to be achieved, while clearly isolating and protecting the Process Control System so that control is possible by only authorized individuals from restricted locations? ~~Must~~Shall the point of entry of process operator control actions be tracked? Do portable storage devices (e.g. flash drives) need to be utilized? If so, what security procedures or precautions will be taken to ensure the control system is not compromised?

2.4 CONCEPTUAL DESIGN ASSESSMENT

The conceptual design process will result in the collection of the needs and desires of all of the interested groups discussed above. The draft conceptual design should be reviewed before it is approved. This review should address:

- Has an adequate cost/benefit analysis been performed?
- Do the requirements meet the project objectives and business goals?
- Have constraints imposed by existing standards and practices been reconsidered against advances in technology and resulting improvements in business value?
- If a new or upgraded technology is involved, has the method of migration of the systems been assessed and any substantial operating impacts identified?
- What impacts are there upon staffing?
- Are there special support requirements that may be beyond the training and capabilities of existing staff?

- Have other human factors such as operator job loading, simultaneous tasks, etc. been evaluated? Are there any significant departures from previous practices and experience?

- Have strategic or mandatory constraints been considered?

3 Process Control Functional Specification

The Process Control System functional specification combines the elements of conceptual design assessment, Process Control System basic functions and the specific requirements of a particular process unit and site together into a document that can be used as the design basis for a project. This document has the following objectives:

- Identification of specific Process Control System functional requirements based upon the conceptual design basis and the general functions described in Section 4.

- Identification of the physical characteristics of the Process Control Systems.

- Identification of the technologies that will be used or considered for use.

These items should be defined in sufficient detail to support development of purchase or bid specifications, and provide a sufficient engineering basis to proceed with detailed Process Control System design, configuration and programming.

3.1 SCOPE DEFINITION INPUT

The Process Control System functional specification is prepared in parallel with other process design activities that are required to adequately identify the costs and benefits of a proposed project. A number of design documents are prepared during these activities that are necessary to support the Process Control System functional specification. These are described below.

3.1.1 Process Flow Sheet and Specifications

The process flow sheet, description and specifications provide the basis for establishing the Process Control System functional requirements. The data contained in these documents assist in defining the size of the Process Control System and the control functions required. The characteristics of the process will also form the basis for identification of requirements for Process Control System security, robustness and speed of response.

3.1.2 Piping and Instrument Diagrams

Process Piping and Instrument Diagrams (P&IDs) form a definitive basis for identifying specific control functions required and development of quantities for the Process Control System. At the time the Process Control System specification is being prepared, P&IDs will still be incomplete, but should be in a state that allows for reasonable definition of functions and quantities and identification of details that still need to be developed.

P&IDs also provide a basis for identifying the basic control functions to be used and the separations between them, such as divisions between continuous control functions, alarming, discrete control and Safety Instrumented Systems.

3.1.3 Plot Plans

Plot plans show the location of all process equipment and significant support facilities such as control centers, satellite control houses or remote instrument enclosures, analyzer buildings, local control equipment, etc. These documents provide the basis for defining the location and approximate quantities of Process Control System equipment and identification of communications system requirements.

3.1.4 Safety Instrumented Systems

Process HAZOPS should have been performed and any needed Safety Instrumented Systems or other protective instrumented systems should have been identified and their integrity levels determined. This activity includes initiating work on the safety requirements specification and supporting documentation.

3.2 PROCESS CONTROL SYSTEM FUNCTIONAL REQUIREMENTS

The Process Control System specification should identify the specific functions of the Process Control System, required performance for each function and the approximate quantities for each function. The answers to the questions posed in Section 2 should be the basis for defining all of the functional requirements for the Process Control System.

Section 4 provides general description of many potential functions. This definition of functional requirements should include all functions required, irrespective of which organization is expected to be responsible for implementation.

Complex control loops should have a functional narrative provided for each application that identifies the objective of the control application, the basic functions and computations required by the application and the process data required.

Special purpose systems such as compressor and turbine control and monitoring systems, complex analyzer systems or similar functions that are not readily performed by the generic Process Control System need to be identified as part of the project scope.

3.3 PROCESS CONTROL SYSTEM PHYSICAL REQUIREMENTS

Process Control System physical requirements cover definition of how the Process Control System is expected to be implemented. This portion of the specification should address scope items such as those listed below. API RP 554, Part 2 provides information on design practices that may be needed to support this information.

- The general physical layout of the Process Control System including the location and approximate layout and size of control centers and satellite control houses and other equipment.

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

- 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 types, general layout and routing of fieldbuses 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.

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

3.4 TECHNOLOGY SELECTION

By the time the Process Control System functional specification is developed, the project organization should have a fairly good idea of what specific process control technologies will be considered, or should be actively evaluating alternatives. The selection of control technology should be based upon achievement of business goals in a cost effective manner.

Consideration of business impacts and drivers is inherent in identifying functions required of the Process Control System. Selection of the Process Control System technology ~~must~~shall be made with these requirements in mind. A review of candidate technologies should be performed to ensure that the following have been addressed.

- Does the technology meet the functional requirements?

- Is the technology consistent with commercial requirements?

- Have the lifecycle cost considerations been addressed in technology selection? This includes training, maintenance and long term operation issues as well as initial costs.

- Has the potential obsolescence of the technologies been assessed?

The technologies under consideration should be reduced to a manageable amount, generally no more than 2 or 3 during this process and be limited to those technologies that meet the business goals.

The selection of control technology can greatly impact the physical layout of the Process Control System and leaving too many alternatives open will degrade the quality of the specification and may require parallel design efforts until a final section is made. Late selection of control technologies can have substantial impacts upon fast-track projects.

If a change in control systems or system technology from existing systems is being considered, the means of satisfying all of the functional requirements in the new system, as well as how the new systems interact with existing systems should be part of the assessment. This will require a rather detailed understanding of the migration paths for the facility and how various groups might be impacted by the transition.

The technology selection for the Process Control System specification should be sufficiently narrow to allow the following:

- Identification of the Process Control System physical requirements identified above.

- Identification of software operating systems applications and quantification of impacts upon design and support costs.

- Identification of basic control technologies, such as centralized systems, fieldbus based systems and identification of major functional equipment such as continuous control, discrete control and Safety Instrumented Systems.

- Identification of system integration requirements between Process Control Systems and other business applications.

3.5 EXECUTION PLAN

The execution plan should identify all of the significant work items required to complete the remaining phases through commissioning of the Process Control System project and who is expected to perform the work. This plan should address at least the following:

- Identify responsibility for design, construction, checkout and commissioning activities.
- Identify responsibility for various design activities, scope items and interfaces for exchange of design or other required information. This identification should closely follow each of the functional requirements such as responsibilities for the basic Process Control System, advanced control systems, historians and data handling and for business systems.
- Identify the transition plan for the Process Control System if one applies. What tie-ins are expected? Will transfers be done on-stream, during a shutdown or a combination of the two? If new technologies are involved, how does the change impact the execution of the project, including issues such as data base conversion, training and system testing?
- Identify plans for implementation, testing and validation of SISs or other complex interlock or sequence systems.
- Identify significant purchases or contracts to be let with expected scope.
- Identification of project schedules showing milestones for significant activities and deliverables.
- Identify the overall management plan, which addresses how all of the entities responsible for the work interact, how schedules are coordinated and information is exchanged and how performance will be monitored.

3.6 OWNERSHIP AND OPERATION PLAN

The impacts of Process Control System selection and design upon the organizations that will own and/or operate and maintain the equipment ~~must~~shall be identified as part of the Process Control System specification. This portion of the specification should consider and identify at least the plan, scope and costs for the following items. These issues are discussed in API RP 554, Part 3.

- Identify technical support personnel required to monitor design activities, test and commission the systems and support and maintain them on a day to day basis.
- Identify quantities and qualifications for maintenance support personnel that will be required to perform Preventative Maintenance, troubleshooting and repair functions.
- Define the level of support which will be available, e.g., day coverage, round the clock coverage, etc.
- Define the split between owner/operator personnel, Process Control System manufacturer or integrator contract support or third party contract support.
- Identify training requirements, schedules and costs for system design, testing, commissioning and day to day support. This plan should address both engineering and maintenance technician requirements.
- Identify spare parts requirements including hot spare and test systems.
- Identify ongoing costs for software maintenance and upgrades.
- Identify long term costs associated with probable hardware upgrades.

- Identify any requirements for specialty support systems such as simulators, training systems or other equipment and software not directly part of the Process Control System.

4 General Functions of Process Control Systems

4.1 INTRODUCTION

This section discusses the functions that are typically performed by Process Control System independent of the hardware and software platform upon which they are implemented. API RP 554, Part 2 addresses recommendations for implementation of these functions using currently proven technology.

Figure 2 illustrates these functions and provides references to paragraphs where each one is discussed. While this figure appears to indicate a specific hardware and software layout, it is not intended to do so. These functions may be organized differently depending upon the actual hardware and software used.

Specific applications may require all or only a few of these functions. The Process Control System functional specification, along with an estimate of actual physical inputs and outputs, then will enable the user to obtain accurate proposals from hardware and software vendors and identify work which needs to be performed by third parties. See API RP 554, Part 3 for guidance on process to develop project costs and schedules.

4.2 SENSING AND ACTUATION

All Process Control Systems require knowledge of process conditions in order to take control action and to display the process conditions to the operator. Process sensors convert process conditions to another physical property usually electrical, suitable for control and indication.

Process sensors provide a signal to the Process Control System that represents the physical state of the process. Sensor types and functions are described in API RP 551 and API 555 and in numerous PIP documents. The means of transmitting sensor information to the Process Control System are described in API RP 552.

The control function determines the action necessary to control the process and sends this information to the actuator of the final element. Actuator and final element information can be found in API RP 553.

4.3 SIGNAL TRANSMISSION

Field devices communicate with the control system through different means based on accuracy requirements, available technology, ease of installation, range of operation, and security, reliability and response requirements. The most common techniques are described in API RP 552 and 4.3.1 – 4.3.3 below. The type of signal transmission used will depend upon the Process Control System being used, a user's infrastructure and the amount of information that is to be obtained from the field instrumentation. The signal transmission systems in common use today are briefly described below.

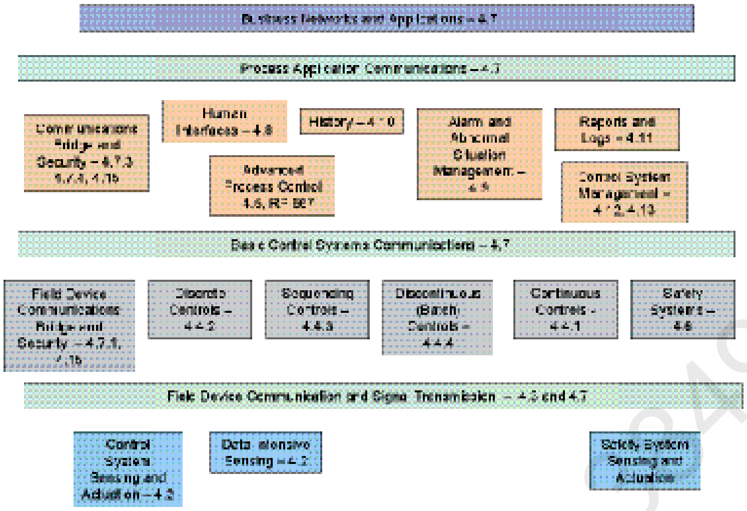
Business Networks and Applications – 4.7
Process Application Communications – 4.7
Communications Bridge and Security – 4.7.3 4.7.4, 4.15
Human Interfaces – 4.8
History – 4.10
Advanced Process Control 4.6, RP 557
Alarm and Abnormal Situation Management – 4.9
Reports and Logs – 4.11
Control System Management – 4.12, 4.13
Basic Control Systems Communications – 4.7
Field Device Communications Bridge and Security – 4.7.1, 4.15
Discrete Controls – 4.4.2
Sequencing Controls – 4.4.3
Discontinuous (Batch) Controls – 4.4.4
Continuous Controls – 4.4.1
Safety Systems – 4.5
Field Device Communication and Signal Transmission – 4.3 and 4.7
Control System Sensing and Actuation – 4.2
Data Intensive Sensing – 4.2
Safety System Sensing and Actuation

Figure 2—Process Control Systems Functions

Comment [PGJH2]: Improve graphic quality. Graphic source is needed. Action by API Editor

4.3.1 Analog Transmission

Analog signal transmission has historically been the common method of signal transmission between a Process Control System and its field instrumentation. This communications method requires dedicated input and output channels and a dedicated pair of wires for each field device and typically uses a 4 – 20 ~~ma~~mA signal to communicate the value of a measured input or a control signal output. No data other than the value of a process variable or the command to a final control device is available.

4.3.2 Analog Transmission with Digital Communications

Some serial communications technologies allow digital signal communications to be imposed on top of a 4 – 20 ~~ma~~ mA signal. This technique allows the Process Control System to operate with an analog transmission system while also allowing parallel devices such as hand held communicators, personal computers or similar devices to communicate with field devices that have such communications capabilities built into them. The communications protocol may be an open protocol such as HART, or a proprietary protocol provided by a field device manufacturer.

4.3.3 Digital Communications

Some Process Control Systems allow for direct digital communications with field devices instead of using analog transmission. These systems may use an open protocol, such as Foundation Fieldbus or Profibus, manufacturer’s proprietary communication system or an industry standard bus system. These designs allow for full access to configuration, performance and diagnostic information functions of field instrumentation. It is also possible for digital communications to be transmitted using various wireless technologies. See 4.14.6 regarding security of wireless communication.

4.3.3 Device Alerts and Alarms

Field devices that support analog-digital or digital communications (e.g. HART, Foundation Fieldbus, Profibus) may provide a variety of device diagnostics information related to device health, communication or transmission integrity, or process conditions. Such diagnostics information may be transmitted from the device to the control system via device alerts or device alarms. (The terms “device alerts” and “device alarms” are often used interchangeably.) Device alerts are different for each instrument and may have different default priory levels and determined by the device manufacturer. Control systems may display these device alerts in either the asset management alert monitoring software, or in the operator interface or HMI. Control systems may need to have the appropriate device configuration files (e.g. device description, DTM, or proprietary configuration files) to properly display the device alerts. Table # shows some example device diagnostics functions that may be displayed in the control system.

Type	Functions
Device Health	Electronics Failure
	Sensor Failure
	Radio Failure (Wireless Devices)
	Supply Voltage Failure (Wireless Devices)
	Supply Voltage Low (Wireless Devices)
	Stuck User Interface Buttons
	Configuration Error
	Incompatible Electronics and Sensor
	LCD Update Failure
	Configuration Changed Flag
	Software Incompatibility Error
	Calibration or Trim Failure
	Transmitter out of specification
	Electrode Coating
Communication or Transmission Integrity	Communication Failure
	Ground/Wiring Fault
	Simulation Active
	Analog Output Saturated
	Analog Output Fixed
	Pulse Output Out of Range
	Analog Output Out of Specification
	Pulse Output Fixed
	Communication Failure
Process Conditions	Abnormal Statistical Conditions
	Rapid Increase in Process Variable
	Plugged Impulse Lines
	Temperature has Exceeded device Limits
	Sensor Out of Range
	High Process Noise Detected
	Empty Pipe Detected
	Reverse Flow Detected
	Process Limits Exceeded

4.4 BASIC CONTROL FUNCTIONS

Basic control functions can be classified as either continuous or non-continuous. Continuous regulatory control functions execute on a user defined interval. The user ~~must~~shall evaluate the interval required for any particular process application. Non-continuous regulatory control functions execute upon events such as an operator action, process condition, alarm or some other event. Non-continuous regulatory control functions include logic control, sequential control and batch control.

Process Control Systems are provided with a set of basic control functions. The implementation of these functions varies with the particular Process Control System, but most basic functions are generally similar. IEC 61131-3 defines standards for control functions and their implementation. While many early Process Control Systems implemented these functions using proprietary methods, recent trends have been for more Process Control System providers to comply with IEC standards, or at least be in great part consistent with the standards.

4.4.1 Continuous Control Functions

Table 2 lists many common continuous control functions that are provided with process control systems. This is not a comprehensive list, and the actual functions available and their characteristics may vary from manufacturer to manufacturer.

Table 3 lists some of the functions that are provided as auxiliary sub-functions to provide enhanced functional selections within the more general functions. See IEC 61131-3 for greater discussion.

A major factor in the performance of Process Control Systems is the controller execution rate. This will impact overall response of the Process Control System to process changes.

4.4.2 Logic

Logic control consists of functions that operate in a discontinuous manner based upon the status of discrete or continuous inputs, and generally have a discrete output that turns on or off a control element, opens or closes a valve, etc. Logic control may exist on a stand-alone basis or may be integrated with continuous control functions.

Table 4 lists a number of logic functions that are typically available. See IEC 61131-3.

4.4.3 Sequential

Step-by-step programming to perform certain sequential operations are useful for many processes. Typically, this type of operation is used for start-up of particular process units or equipment within those units. For example, sequential control may be used for a regeneration process or as part of a start-up or shutdown system.

Sequential control applications can be implemented by ladder logic, function blocks, sequential function charts or a specific batch oriented programming language. Ladder logic has historically been used to implement sequential control functions, but applications are difficult to document and maintain. Function block and sequential function charts are a graphical method of linking specific operations into a sequence of operation. These applications are self-documenting and more simple to troubleshoot. Batch oriented programming languages can offer flexibility in implementation, and are easily documented and maintained. See 4.4.4 for discussion of batch applications.

4.4.4 Batch

A special requirement of batch applications is the need to program each specific batch by batch formulation and the equipment being used to produce it. The ability to change the batch specific parameters should be available to the operator although the security to change these parameters should be specified in the design documentation. Batch control may utilize continuous, discrete and sequence control. Some applications may also require batch tracking and records of raw materials, batch conditions and final product properties to be kept by the batch control system.

The U. S. standard ISA S88.01 for batch control systems, and its IEC equivalent IEC 61512-01, have become two of the most widely adapted standards for manufacturing control systems in the U. S. and Europe. These standards define a common set of models and terminology that can be used to describe and define process-manufacturing systems. The models emphasize good practices in the design and operations of these systems, and a supporting methodology called "Modular Batch Automation" has been developed to codify the good practices. The standard has been effectively applied in continuous production, where it is used to define start-up, shutdown, changes in product mix, changes in raw materials, and changes in production rates.

The ISA S88.01 standard defines a separation of product information from production equipment capability. This separation allows the same equipment to be used in different ways to make multiple products, or to perform different operations on the same equipment. The key reason for this separation is to make recipe development straightforward enough to be accomplished without the services of a control systems engineer.

Table 2—Continuous Control Functions

Type	Functions	Comments
Input Characterization	Analog input conversion, linearization, square root extraction and scaling	
	Automatic validity test and alarm (out-of-range limits)	
	Totalize analog input and pulse count input	
	Contact status	
Output Characterization	Output scaling-includes output signal range (4 – 20 milliampere, 1 – 5 volts, etc.)	
	Output characterization—includes scaling for split range controllers, and non-linear characterization of outputs	
PID Functions	PID Basic Controller	The PID control functions should be based upon the overall requirements to limit the variability of the controller against the set-point. A major factor in the performance of the control system is the controller execution rate. Also, some applications require the controller algorithm to operate off of the error or the measured variable or a combination of these. For example, operating off of the measured variable eliminates the "proportional bump or kick" that results from a set point change.
	PID Ratio	
	PID Cascade	
	PID Bias	
	PID Differential Gap	
	PID Adaptive Gain	
	PID Non-linear	
	Manual Station	
	PID Self-tuning	
	External Output Tracking	
	Reset Limiting	
Math Functions	Add	Seamlessly integrating these functions within the control library should be accomplished so that the overall performance of the control loop is not adversely impacted by their use. For example some math functions may interrupt controller balancing functions for bumpless transfers.
	Subtract	
	Multiply	
	Divide	
	Summation (bias)	
	Difference	
	Square Root	
	Square	
	Absolute Value	
	Logarithm (common and natural)	
	Exponential	
	Polynomial	

Limit Functions	Low Select	
	High Select	
	Low Limit	
	High Limit	
Dynamic Functions	Lead/lag	Used to mathematically model process dynamics.
	Dead Time	
	Velocity Limit	
	Totalize	

Table 3—Auxilary Control Functions

Type	Functions	Comments
Miscellaneous Functions	Bumpless Transfer	These functions are generally incorporated within the options available for configuration within other control functions. For example, a PID algorithm may have these capabilities, which can be activated by user configuration.
	Ramp of Set Point	
	Ramp of Output	
	Ramp of Calculated Values	

Table 4—Logic Functions

Type	Functions	Comments
Logic Control	And	Configurable logic and sequential functions may be provided in order to perform complex interlocking, counting, event sequencing, and other logic (Not, And, Or) calculations. Logic should be displayed in a readable form such as ladder diagram, function block displays, or Boolean statements.
	Or	
	Exclusive Or	
	On/Off Delay	
	Inverter	
	Flip-flop	
	Pulse	
	Time Delays	
	Counters	
	Compare	
Input/Output	Discrete Input	Functions to read inputs and write outputs and control associated signal conditioning, diagnostics or other input/output functions.
	Discrete Output	
Operator Interface	Status Display	Functions that make status and values within the logic available to operator displays and which allow the operator to issue commands and settings to the logic.
	Value Display	
	Operator Command Display	

4.5 ADVANCED CONTROL FUNCTIONS

Advanced control functions are those control functions that are beyond the functions commonly associated with regulatory control systems. Advanced control functions may be characterized by any of the following:

- A control function that controls or manipulates multiple variables in order to maintain one or more operating objectives.

- A control function that performs calculations beyond those available from regulatory control functions.

- A control function that may utilize a significant number of regulatory control functions connected together in a complex manner.

- A control function that is executed in a higher level computing resource such as a process control computer, or in a programming environment of a lower level computing device, irrespective of the complexity of the computations.

API RP 557 describes the functions and implementation of advanced control systems.

4.6 SAFETY, PROTECTIVE AND PROCESS INTERLOCK SYSTEMS

This section discusses the general functionality of discontinuous controls that are required for safety, protective and process interlock systems. The discussion identifies the basic principles of the identification of various types of safety applications, and the additional procedures and design considerations required for those applications that have safety functions. Specific design considerations for the implementation of such systems are given in API RP 554, Part 2. Recommended practices for safety and protective systems in gas fired heaters are given in API RP 556.

The general categories into which these functions fall are described below. Applications that are categorized as safety functions fall under the regulations described below and are generally considered to be outside the scope of a Process Control System.

Applications that are not classified as safety applications may be considered for inclusion in the scope of the Process Control System, or included with the safety systems, depending upon the user's determination of the required level of integrity. If this is done, care should be taken. If non-safety applications are mixed with safety applications, the non-safety applications may have to be administered according to the safety system procedures.

Safety and protective systems can have one or more basic functions which determine the methods that ~~must~~shall be used to specify design and maintenance requirements and which will affect whether the functions may or may not be implemented within the Process Control System.

4.6.1 Safety Instrumented Functions

Safety instrumented system functions are generally intended to minimize the potential for loss of containment and the consequences thereof. Local regulations and industry standards such as ISA/ANSI 84.00.01 (IEC 61511 Mod) and IEC 61511 and IEC 61508 govern the scope and design of safety instrumented systems. PIP PCESS001 provides additional information on application of these standards.

The need for safety instrumented functions is normally established through a hazard analysis process based upon either quantitative or qualitative measures of acceptable risk associated with a process and its potential hazards. During this process, potential hazards are identified and various layers of protection are applied to reduce the likelihood of that hazard occurring. If sufficient layers of protection cannot be identified to reduce the risk the process hazard to an acceptable level, then safety instrumented functions, with an appropriate integrity level may be necessary to achieve that end.

4.6.2 Environmental Protective Functions

Environmental protective functions are intended to minimize the probability that operation or malfunction of a process will cause unacceptable environmental pollution or other environmental damage. An environmental protective function may perform any number of functions, but common functions are to shut down major processing equipment, or to interlock equipment so a situation that could result in significant environmental impact does not occur.

4.6.3 Asset Protective Functions

Asset protective functions are intended to minimize the probability of financial loss, e.g., due to equipment damage, excessive loss of production or contamination of products. An asset protective function may perform any number of functions, but common functions are to shut down major processing equipment, or to interlock equipment so a situation that could result in significant economic loss does not occur.

4.6.4 Process Interlock Functions

In some process applications, the complexity and time available to react to an abnormal condition in the process such as high level or low flow requires an operation override to be installed. The interlock is designed to take the unit to a predetermined state upon the abnormal situation. Other interlock functions automate functions and/or operational sequences that would otherwise have to performed manually, such as valve switching associated with batch or semi-batch operations. These applications generally do not require the same integrity levels that the other functions listed above do. Often, these functions are performed within the scope of the Process Control System.

4.7 CONTROL SYSTEMS DIGITAL COMMUNICATION FUNCTIONS

Process Control Systems make extensive use of digital communications at all levels of the system. Security and data loading issues usually result in a multi-layer network structure; however the exact configuration is dependent upon hardware, the data applications, software and security requirements. See API RP 554, Part 2 for discussion of implementation. The general functional communications that exist in a Process Control System are outlined below.

- A field device communications level that allows communication with and among smart field devices. This level allows for configuration of field devices and controls, communications between field devices and communication with other process control modules and HMIs, usually through an interface to a process control communication level.

- A process control communication level that is generally used for process control modules to communicate with one another and with HMI, historian and advanced control functions. This communication level may also pass values, messages and other data to and from field device communications.

- A plant information communication level that is generally used for process control modules, HMIs, historians and advanced control functions to communicate with each other and with business level communications. This communications level is also generally used to allow multiple Process Control System areas to communicate with one another.

- Communications to or from external systems to the Process Control System for special purpose devices such as machinery monitoring systems that are provided for diagnostic or other support functions.

- Business level communications that provides connectivity to general purpose networks such as corporate or external LANs or WANs, including communications with general purpose desk top computers.

As mentioned above, these communication functions may be implemented in various ways, using a variety of communication technologies. API RP 554, Part 2 describes a number of common implementations of these communications functions.

4.8 HUMAN MACHINE INTERFACE

4.8.1 Basic Function

All Process Control Systems ~~must~~shall include an HMI that provides displays of process conditions and control system status, as well as allowing for operator entry of commands, annunciation of alarms and display of historical charts and reports.

The operator consoles should provide both preformatted displays and custom graphic displays. The preformatted displays should be designed to allow easy setup and maximize communication of data to operators and engineers.

Display designs should allow the operator to access information and initiate any action in an uncomplicated, effective manner. Display design requires input from unit operation representatives and other responsible management. Displays as described in Table 5 should be provided.

EEMUA 201:2003 provides an extensive discussion of HMI related issues. The publication identifies the following categories of operation which need to be considered in HMI design, in the order of their importance:

Category 1	Abnormal situation handling—This includes start-up and shutdown.
Category 2	Normal operation—Most utilized role.
Category 3	Optimization.
Category 4	General information retrieval.

The operator consoles should provide both preformatted displays and custom graphic displays. The preformatted displays should be designed to allow easy setup and maximize communication of data to operators and engineers.

Table 5—Human Machine Interface (HMI) Displays

Type	Description
Overview	Overview displays are used to indicate the status of the plant process and equipment by highlighting specific areas of deviation from the normal operating envelope. Operator control actions are typically not required from this display, however appropriate links to other displays should be provided to facilitate corrective actions by the operator.
Faceplate	Faceplate displays indicate parameters associated with a given tag, including process variable, set point, alarm status, and provide access to related control functions.
Detail loop	Detail loop displays should be provided for each control point and should show the various parameters that are pertinent to that point, including auxiliary data such as the source of inputs to the point, tuning variables, and alarm set points. It should be possible to tune control functions from these detail displays under a protected status.
Trending	Trends display any selected data stored in the history system. This data may be real time or historical. It should be possible to trend multiple variables on a single display. Operator ability to change on-line, scaling, color selections, and the time period viewed should be available. It is often beneficial to combine trend displays with group or graphic displays.

Custom graphic	Any point, measured or calculated, should be capable of being displayed on a custom graphics display as an active variable. The operator should be able to manipulate any control loop, device, batch procedure, and so forth, from a graphic display. The graphics package should allow the user to define a library of symbols, including dynamic behaviors. It is desirable to have linkages from a graphic display to other graphic displays, so that the graphic displays can be accessed from one to another with a minimum of steps.
Utility	Utility displays should show the status of all system functions.
Diagnostic	The complete system should have on-line diagnostics sufficient to identify failures to the module and/or card level. Displays should provide English explanations of the problem and not merely an error code number.
System status	A system status display on the operator’s console should summarize the status of each of the components connected to the system. Failures or a switch-over to a backup unit should be shown on the system status display. This display should provide sufficient information to indicate the type of failure detected, and the operator shall be advised of a failure by an audible alarm.
System configuration	System configuration displays should provide information about the configuration of system hardware and software. These displays generally allow authorized users to set up system parameters.
Engineering	Engineering displays allow configuration of the control, computational, and logic functions of the system. Access to the displays should be a protected function. Configuration may be able to be performed in either on-line or off-line modes. Typical functions available from these displays are: • A display which shows the titles of all display groups available. • A display which shows all tag names, numbers and groups to which they are assigned. • Development of all process graphics and user defined graphic displays. • Development of application programs and debugging of the programs. • Database setup, query, reporting and similar functions. • Security definition and monitoring.

4.8.2 HMI Displays

Display designs should allow the operator to access information and initiate any action in an uncomplicated, effective manner. Display design requires input from unit operation representatives and other responsible management. Displays as described in Table 5 should be provided.

4.8.3 Design Factors

Design of an HMI system ~~must~~shall consider a number of critical human engineering issues. Among these are:

- Number and size of display screens.
- Display of concurrent data and multiple windows per display screen.
- Navigation of displays including display hierarchy and access to critical displays such as process alarms.
- Display design practices, format, layout and standards.
- General control center design including lighting, ambient conditions, work area, etc. See API RP 554, Part 2 for control center design practice recommendations.

EEMUA 201 discusses many aspects of the above items in some detail.

4.8.3 Digital Field Device Interfaces

Many field devices provide multiple process variables, device health, or other advanced diagnostics information via digital communications (e.g. HART, Foundation Fieldbus, Profibus).

Often, it is desirable to display this information in a form that is easily recognized and understood by the person using the field device (e.g. engineer, operator, maintenance). Device manufacturers may employ human-centered design principles to develop easy-to-use interfaces to digital instruments. Such interfaces may include one or more of the following:

- A device overview or dashboard screen showing the most important variables or parameters associated with the device.
- Visual representation (e.g. dial gauge, bar graph, or trend over time) of process variables or other numerical values provided by the field device.
- Visual indicator of device status (e.g. good, advisory, maintenance, failed)
- Guided methods or setup wizards that direct the user step-by-step through common configuration tasks
- Shortcut buttons for accessing the most common configuration tasks
- Detailed help associated with device alert or device alarm conditions

Multiple technologies exist to allow development of digital instrument interfaces. The most commonly used technologies are EDDL and FDT/DTM. EDDL (Electronic Device Description Language) is a text-based descriptor language. FDT (Field Device Type) / DTM (Device Type Manager) is a Microsoft Windows-based COM or .NET interface platform. An advantage of EDDL is that because it is text-based, it is not dependent upon any particular operating system (e.g. not tied to Windows), so it can be used by any host system that has implemented the rules for interpreting the EDDL language. An advantage of FDT/DTM is that Windows application code can be embedded in the DTM, and so it may be possible to create user interfaces that contain more extensive functionality than could be defined with EDDL. Conversely, because FDT/DTM is built on the Windows COM interface, it is not possible to use this technology on any non-Windows host system.

Most device manufacturers create a device description (DD) and a DTM. Both technologies define the parameters available in a field device (configuration, measurement, status), and how those parameters are displayed to the user. The DD or DTM for a given field device type ~~must~~shall be loaded into the host system DD's are used in control, asset management, and handheld hosts. DTM's are used in asset management hosts or standalone PC based stations. The host system uses the appropriate DD or DTM corresponding to a field device whenever the user-interface needs to be displayed.

When specifying an automation system, an owner-operator should determine which digital device interfaces will be utilized within their facility, considering both present and future needs. An owner-operator may ask an automation vendor which digital device interfaces their system(s) support, and utilize this information in determining the selection of their automation system.

4.9 ALARMING

4.9.1 General 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 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.
- Record events and changes for historical record purposes.

The capabilities of Process Control Systems have made what was once a relatively simple function into what can be a complex and sophisticated subject. API RP 554, Part 2 contains greater description of alarm functions. Documents published by AIChE[7] and EEMUA also contain extensive descriptions of alarm systems. The descriptions in this recommended practice are generally directed to alarm functions for Process Control Systems which use shared display operator interfaces. See ISA 18.1-1979 for a description of physical annunciator systems.

Many systems also provide software for alarm analysis which can identify repetitive or duplicate alarm functions.

4.9.2 Non-process Alerts

The communications and functional capabilities of Process Control Systems make many business related alarms and alerts possible. For example it may be desirable to provide alerts associated with operating economics, operation of advanced control applications and other events not necessarily associated with process operating safety or protection of assets. This class of alarm also includes alarms and alerts associated with the operation of the Process Control System to inform the operator of diagnostic faults or equipment failures associated with the control system. In newer systems, alarms and alerts associated with field instrumentation may also be available.

Environmental regulations also can place significant operating constraints upon operations or require responses from operators that are not necessarily production or safety oriented.

Functional specifications for a Process Control System should address the use of business and environmental related alerts and differentiate the methods that are used to alert the operator of these conditions versus those used to alert the operator of required responses.

It may also be required that alarms or alerts associated with diagnostics associated with equipment health monitoring or environmental performance be directed to personnel other than operators such as maintenance staff monitoring equipment for predictive maintenance purposes or other staff who review environmental performance monitors. Additional alarm and alert functionality may be necessary to enable these functions.

4.9.3 Alarm Management

The alarming capabilities of Process Control Systems can result in excessive alarms and alarm saturation during start-up, upsets and shutdowns. EEMUA 191 contains an extensive description of alarm selection and management topics intended to maximize the value of process and other event alarms. Some of the topics addressed in EEMUA 191 include:

- Alarm risk evaluation and classification.
- Alarm types and prioritization.

[7] American Institute of Chemical Engineers, Center for Chemical Process Safety, 3 Park Ave, 19th floor, New York, New York 10016-5991, www.aiche.org/ccps.

- Alarm system performance.

- Alarm management programs.

4.10 HISTORY

The Process Control System should have capabilities to record, recall and report on the historical performance of the control system and the process that it is controlling. The general trend in history functionality is to minimize the use of paper records and keep as many records as possible in electronic format. Historical data records need to be retrievable. Presentation of historical data is described in 4.11, Reporting and Logging.

One substantial aspect of historical data collection and storage is the generalized use of open system databases to store many or all historical data records. This practice allows extremely flexible and valuable use of the data, as the user is no longer restricted to tools and functions provided by the control systems or historian vendor. Most systems support use of tools such as Standard Query Language (SQL) to search and report on the database contents, and export the search results to a wide variety of external applications and paper or electronic reports.

As open system databases are used, data security becomes a major issue. The implementation of historical databases ~~must~~shall be such that only authorized applications can write to the database, and that unauthorized users cannot bypass system security to modify data records. Data query functions ~~must~~shall be implemented in such a manner that queries and data manipulation is done on copies of the source data and that the source data is protected from corruption due to poor or failed data queries.

4.10.1 Historization of Process Values

Historization of process values is electronic storage of the values of designated process measurements, computed values, or other similar values at designated time intervals. While historization of process values appears to be a straightforward function, there are many associated issues that ~~must~~shall be addressed when the required functions are being defined.

4.10.1.1 The frequency of process value recording needs to be determined. The frequency of data acquisition should be variable, and should be able to be independently specified for each value that is being historized. The method of data recording ~~must~~shall be evaluated and defined. For example, historization software may record snapshot values at the defined intervals, or may record an average of the process value over the defined interval. The method of recording should be able to be independently defined for each value being historized.

4.10.1.2 The methods of history data compression need to be understood and evaluated against the business and regulatory requirements for the Process Control System. There are a number of compression schemes available. Some of these schemes may be acceptable for operational data, but may not be acceptable for data that ~~must~~shall be historized for regulatory reporting. Typical schemes that are used are:

- Short-term storage of process data histories that are sampled at short (1 to 5 seconds) sample intervals and kept in the historian for relatively short periods, such as 12 to 24 hours. This data is typically used by operations and engineering personnel to monitor the process and identify control system tuning or design problems. After the data ages beyond the maximum storage time it is either overwritten, or copied to a longer-term historian as longer time snapshots or averages, typically on a one-minute interval.

- Storage of snapshot data or data averaged over a sample period for some relatively short period of time (e.g., one minute snap shots are stored for 30 days of data). As data becomes older the shorter time period data is averaged into longer time periods, such as after 30 days, one minute data is averaged over 5 or 10 minutes, and data older than 90 days is averaged into hourly averages. The disadvantage of this scheme is that dynamic responses of process values are lost as the data becomes older.

- Storage of process value data using a compression scheme that is based upon saving data samples when the process value changes by some threshold value. This scheme may be combined with snapshot or short time period averaged data for recent historical data (1 to 30 days) and then have the compression scheme applied to older data.

4.10.1.3 In some applications, such as regulatory history, the potential for lost or missing data should be avoided. The Process Control System should have provisions in its design to minimize the loss of historical data while the data historian may not be operating or if communications with the historian are interrupted. Many Process Control Systems have the ability to store limited amounts of data at the regulatory control level and many historians have the ability to recall this data when they are restarted or communications are restored.

4.10.2 Batch and Production Records

Batch and sequential oriented processes present unique needs for collection of historical data. In general, these requirements involve tracking process data for each batch and lot of material produced, equipment used and generic and specific recipes employed. Batch and lot reports that associate all process data with a specific batch and/or lot of product are required for systems that utilize batch control systems.

Batch processes also can require that a variety of recipes and specifications be kept for various products and equipment configurations. The Process Control System should be capable of tracking changes to each recipe.

4.10.3 Regulatory History

Various environmental or other regulatory agencies require data collection and archiving to demonstrate compliance with the applicable regulations. Failure to collect these environmental data or loss of the data can result in significant legal penalties. These requirements can justify a secure system employing mirroring, retrieval, and information database hardware. In some cases, a separate environmental historian and data reporting system may be necessary.

4.11 REPORTING AND LOGGING

4.11.1 Reports

Historical data reports allow for paper or electronic query and reporting of historical process and event data. A historical data reporting system should allow the user to specify a set of values and a time period for data retrieval. Current technology reporting systems should be capable of providing a number of pre-defined reports and provide a means for the user to develop ad-hoc reports.

The historical data report system should provide functionality to export historical data search results to standard software tools where the data may be further manipulated. The functions should be available for any standard system searches as well as ad-hoc and customized searches.

4.11.2 Event Logging

Most control systems display numerous discrete statuses and events that may not be used to initiate alarms, but which often have significance in evaluation of process or system performance or for incident evaluations. The historical performance of these events should be recorded in an event journal that can be queried to support the above evaluations. Event journals should include such events as:

- Equipment status and changes in status.
- Disabling of alarms.
- Operator changes and commands.
- Changes in control system operating states and non-alarmed diagnostic messages or events.

4.11.3 Analysis Tools

The historian should provide tools that allow analysis of events leading up to plant upsets. Some of the features of these tools could include:

- Plots of number of alarms and number of operator actions on the same time scale.
- Selection of time windows and capture of events and alarms during this window.
- Sorting of alarms by type, unit, equipment, etc.
- Sorting of events such as operator action, interlocks, trips, etc.
- Plotting of other process data (T, P, F, etc.) along with alarms and events for a given window.

4.12 SYSTEM MANAGEMENT TOOLS

A Process Control System ~~must~~shall be provided with tools that allow for management of system configuration and software. The tools necessary are typically:

- Configuration tools for control system function definition.
- Configuration of data acquisition and history functions.
- Configuration of operating graphics and other display functions.
- Configuration of alarm functions.
- Network management tools that allow for addition, deletion or modification of devices on the control network.
- Storage facilities for backup of system configuration data.
- Logging functions that record system configuration changes.
- Monitoring tools that allow for monitoring of the performance of system communications and the performance of individual devices.
- Database management tools that allow for the historical or current databases to be maintained.

4.13 DATA BASE MANAGEMENT

One of the results of the advances in application of digital functionality and communications to Process Control Systems is a proliferation in data that ~~must~~shall be managed at all levels of the Process Control System. The sources of this data are varied and may be generated by a number of manufacturers and systems providers and will usually not be integrated. Figure 2 presented an illustration of the overall functionality that may be included in a Process Control System. Figure 3 presents a similar view of this from a data perspective. This figure is intended to be illustrative of the data that may be contained in a Process Control System. The actual data may vary from system to system.

4.13.1 Field Device Data

Most modern instrumentation is operated by some form of microprocessor and has some amount of configuration data associated with it. This data may be as simple as configuration ranges and signal conditioning specifications, or may be substantially more complex. Complex instruments such as analyzers may have a substantial amount of programming associated with their operation.

The primary storage location for this data is within the instrument itself. However, all but the simplest digital instrumentation has some type of configuration program available, usually intended to operate on a laptop PC. These configuration programs also usually have facilities to save copies of the configuration data onto the computer's hard drive and to restore configuration data to a repaired or replaced instrument.

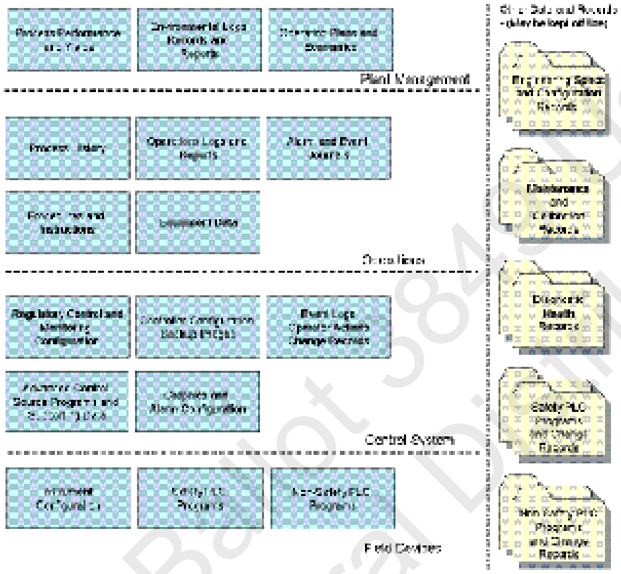
Process Performance and Yields
Environmental Logs Records and Reports
Operating Plans and Economics
Plant Management
Process History
Operations Logs and Reports
Alarm and Event Journals
Procedures and Instructions
Equipment Data
Operations
Regulatory Control and Monitoring Configuration
Controller Configuration Backup
Event Logs Operator Actions Change Records
Advanced Control Source Program and
Graphics and Alarm Configuration
Control System
Instrument Configuration
Safety PLC Programs
Non-Safety PLC Programs
Field Devices
Other Data and Records - (May be kept off line)
Engineering Specs and Configuration Records
Maintenance and Calibration Records
Diagnostic Health Records
Safety PLC Programs and Change Records
Non Safety PLC Programs and Change Records

Figure 3—Process Control System Data

Comment [PGJH3]: Improve graphic quality. Graphic source is needed. Action by API Editor

Field device configuration data and configuration software is often proprietary to the instrument manufacturer and individual device. In these situations, master copies of configuration software and configuration data ~~must~~shall be managed to ensure that accurate data is retained and is available for repairs and replacement.

Adoption of field device communications, particularly the protocols and busses described in 4.3.2 and 4.3.3 have resulted in many more field instruments being capable of being configured from a common software platform. This capability results in substantial improvements in management of configuration software and configuration data. These functions are by no means universally available and each operating facility will still have to manage devices which require proprietary software

4.13.2 Field Device Maintenance and Performance Records

Use of bus technologies has enabled automatic or semi automatic collection of field device test, calibration and maintenance data and storage of this data into a common data base with configuration data. A limited number of software packages are available that incorporate performance definitions from a number of manufacturers that adhere to a common communications standard.

Field device maintenance and performance data will generally capture the results of an event, and the software supporting these functions generally will allow a user to recall and report on single or multiple events. Records may be kept on events such as:

- Changes in device configuration data.

- Test data such as configuration checking or testing of control valve performance characteristics.

- Diagnostics or other alerts detected by configuration or performance monitoring functions.

- Manually entered data describing a manual configuration, calibration, testing or other repairs.

4.13.3 Control Systems Configuration Data

Process Control Systems normally provide extensive functions to store data associated with the configuration of the control system. This data is generally stored on one or more central storage modules that provide hard disk or other storage media.

Data that is typically stored by a Process Control System includes:

- Configuration data for the Process Control System network including types, addresses and other data required for each node and general Process Control System operating parameters and options which have been selected for the system.

- Configuration data for individual controllers, indication points, alarm and status points, etc. This data typically does not include dynamic data such as process measurements and states or controller set points and tuning parameters.

- Data required to define system graphics, customized graphics, reports and other displays that are specified by the user.

- Point-in-time images of various control and input/output modules. These files are generally complete images of the contents of the memory of these modules and include values of dynamic data at the time the image was taken.

- Records of configuration parameter changes.

- Source code and compiled images of custom programming for special Process Control System functions such as computations, advanced control applications, etc. This may also include configuration data for general purpose model-based controllers.

- Records of other changes made by operators or engineers such as set point changes, controller tuning, alarm mode adjustments, etc.

4.13.4 Configuration Data Management

Tools for configuration management allow the user to perform a number of Process Control System point and function configuration activities. These functions usually are associated with the contents of control modules that are directly associated with control and data acquisition functions. Higher level functions and historians usually have their own tools. These include:

- Development of initial configuration of Process Control System functions and I/O. Many of these tools allow for bulk downloads of common data from files prepared off line rather than requiring individual data entry for each point or function.

- Saving of configuration data to backup files. These functions may save images of the controller, individual point and function data or both.

- Export of configuration data to applications that allow for convenient reporting of Process Control System configuration data, management of spare I/O and control function resources and other functions not directly associated with maintaining data loaded into the control system.

4.13.5 Archival Storage and Retrieval

All process historical data, configuration data records, event logs, etc. which are electronically recorded should be routinely saved to an archive located in a safe location. The Process Control System should have tools that allow for simple generation of archive files, and for restoration and query of the archived data.

4.14 SECURITY

Process Control System security has developed into a major concern as technologies move from closed proprietary system designs to open systems that use commercially available operating systems and software. Security is an extremely complex subject and generally accepted practices are still being developed by the industry. The discussions that follow are intended to identify various issues and approaches, but specific implementation recommendations are beyond the scope of this document.

4.14.1 General Issues

A well designed Process Control System will be highly reliable and perform numerous functions that allow the process operator to safely run a process, and to protect against upsets and failures within the process. However, Process Control Systems are directly connected to process sensors and control elements and have the potential to cause substantial hazards, loss of production and other economic loss if they are misapplied or fail to perform their intended functions. Security functions within a Process Control System provide protection against unintentional or intentional modification or operation of the system.

It ~~must~~shall be noted that the primary power of a Process Control System is its flexibility and ability to be applied to an extremely wide range of applications with a minimum of customization. Process Control Systems are real-time systems where prompt response to process demands and presentation of data to process operators is a critical function. Robustness and reliability is also of absolute importance. Security functions of a Process Control System ~~must~~shall not compromise any of these critical functions. A security system that results in reduced response time or reliability can result in exposures and losses which may be of higher probability to cause real personnel or economic loss than postulated problems caused by unauthorized changes or operation.

4.14.2 Physical Security

The most fundamental security aspect of a Process Control System is its location and isolation from areas that are readily accessible by persons who do not have authorization to operate or modify the Process Control System. Some of the characteristics of physical security are:

4.14.2.1 Location within a facility that limits general access to employees or others having specific business within the facility. Most refinery and chemical facilities have basic plant security that is designed to prevent entry into the facility by unauthorized personnel.

4.14.2.2 Ensure that Process Control Systems are continuously attended by personnel that are trained and authorized to operate the systems and monitor the process that it is controlling. These personnel are a layer of protection against unauthorized persons from mis-operating or modifying the control system.

4.14.2.3 Physical isolation of process control equipment in locked rooms or cabinets that have restricted access. This includes restricting physical access to unattended stations that may be used.

4.14.2.4 Prevention of operation of unattended stations by key locks or password protection of the station itself.

4.14.3 Software and Configuration Security

Software and configuration security consists of those functions that determine the level of access to the Process Control System program and data functions through operating and engineering interfaces. Normally this security is implemented with physical key-locked switches or passwords and user accounts or a combination of both.

Normally access to the Process Control System configuration and data is split into several levels, with increasing access to configuration, programming and key system functions at each level. Key lock based systems generally have more limited security functionality as compared to user ID/password based systems. The user ID based security systems allow more flexibility in defining functions available to each user and tracking of actions performed by that user.

General access levels are described below:

4.14.3.1 View Only

View only access is normally the default access level. At this level a user may be able to view the current status of the Process Control System and most of the control and indication values. At a view only level, no manipulation of the controllers or any parameters are available. Access to process graphics may or may not be available.

4.14.3.2 Operating Areas

Most modern Process Control Systems are capable of controlling a number of process areas within the same system, and may consist of several separate operating areas. The Process Control System should have functions that allow specific points to be assigned to specific operating area, and that manipulation or changes to those points should be allowed only by stations that are logged onto that area. Key or user ID and password access should control logging a station onto an operating area.

4.14.3.3 Operator Adjustments

Operator adjustable parameters are those items that commonly require manipulation by an operator as a part of routine operations. These functions include functions such as:

- Adjustment of controller set points.

- Changing of controller modes and manual adjustment of controller outputs.

- Enabling and disabling of alarms.

- Adjustment of low priority or operator convenience alarm set points.

- Changing of discrete point states such as motor and valve commands or other points used to manipulate control functions.

The control system security functions should allow an operator to only change those points which are assigned to the operating area which the station is logged onto.

4.14.3.4 Adjustable Parameters

There are many adjustable parameters within a Process Control System to which a user may wish to restrict access. Functions to define access levels for these types of parameters should be available. Parameters that fall into this category are:

- Controller tuning constants and other functional parameters such as ratios, filter time constants, etc.

- Input and output ranges and limits.

- Calculation block constants.

- Soft alarm set points.

- Alarm priorities.

- Alarm enable, disable, suppress, inhibit and other alarm parameters such as dead bands, anti-chatter delays, etc.

It is preferable to be able to define access levels independently for each of these types of parameters, and desirable to set greater restrictions on a point-by-point basis. This functionality is not available in all Process Control Systems, so the user ~~must~~shall evaluate a particular Process Control System's security in this area and develop a security plan for management of change for these types of parameters.

4.14.3.5 Control Configuration and Programming

Control configuration is generally thought of as the process of defining how available standard functions (PID, inputs, outputs, calculation blocks, etc.) are connected together, what sub-algorithms should be used, and what the value of their various parameters should be. Programming is generally a high level function that involves development of custom code to perform functions that cannot be implemented using standard functions. Other functions that fall under this general category are development of display graphics and reports.

Access to these functions should be restricted to properly qualified and authorized personnel. Usually, a key lock or a user ID/password security system protects these functions. Some Process Control Systems further restrict access to these functions by requiring that they be performed at stations that are specifically designed or configured for them.

4.14.3.6 System Configuration and Parameters

System configuration functions and values of parameters that affect system behavior and performance should have the highest level of security available assigned to them, and only a few key support personnel should have access to these functions. In some Process Control Systems, system configuration functions may only be accessible through a dedicated engineering interface.

4.14.4 Intra-system Communications

Many large Process Control Systems have the capability for several control networks to be connected together, either directly through gateways, or indirectly though a process information network. Intra-system communications are normally regulated by system software which limits the manner and quantity of information exchanged. Intra-system configuration ~~must~~shall be carefully examined to make sure that the security of these communications is adequate for the application. Some issues that should be evaluated when considering the acceptability of intra-system communications are:

- How is the system configured? Are messages tightly controlled by Process Control System software design or are open system techniques used?

- What provisions are made to ensure that devices located on another local network or outside the Process Control System cannot make unauthorized writes to process control equipment using the intra-system communications?

- What types of data and messages can be communicated across the intra-system communications path? Is the communications path used only to read data from another local network or are data writes or changes in engineering or system configuration data allowed?

- How does the Process Control System respond if intra-system communications fail?

4.14.5 Communications to Other Systems

A major function allowed by newer technology Process Control Systems is very powerful and open communications paths and techniques to communicate with outside systems including devices located on business LANs or WANs or through the Internet using VPNs or other types of connections. Many of the security concerns for intra-system communications are magnified for communications with outside systems since the potential for unauthorized and damaging communications are substantially increased.

Communication paths to outside systems should be highly regulated to prevent unauthorized messages and instructions. Some functions that should exist are:

- Direct communications between outside systems and devices connected to the process should not be allowed. All communications with outside systems should be routed though modules that buffer all communications and prevent viruses or hacking attempts from passing through the buffer systems.
- Communications between computers that perform process control functions and outside networks, such as business networks or other computers located on the process control network (such as those performing field instrumentation configuration and performance monitoring) should be tightly controlled with multiple levels of security such as a combination of hardware and software based fire walls, DMZs and tightly controlled application communications.
- Access to process control networks by wireless devices should be controlled and encrypted.
- Access to process control networks by flash drives should be done using precautions and procedures which ensure that the control system is not compromised.

4.14.6 Wireless Communication

Wireless communication has many advantages such as lower installation costs, ease of expansion, faster commissioning and others. Each wireless application should use appropriate design and implementation practices for its technology to ensure robust and reliable long-term operation.

Formatted: Font: (Default) Arial, Character scale: 100%, Condensed by 0.1 pt

API RP 552 *Transmission Systems* shall be used for Wireless communications.

Formatted: Condensed by 0.1 pt

Formatted: Font: Not Italic

Formatted: Font: Not Italic

Formatted: Condensed by 0.1 pt

~~The majority of the wireless applications employ ISM based, 2.4 GHz or 5.8 GHz IEEE standard radios for the physical layer.~~

~~Typical wireless applications fall into a small set of classes:~~

- ~~Wireless Plant Networks: These networks provide WiFi or IEEE 802.11a/b/g/n wireless access points for multiple applications. Those applications include but are not limited to: 1) mobile worker or operator, 2) video surveillance, 3) data backhaul. These networks provide standard security mechanisms and high data bandwidth. These networks are typically used for monitoring and supervisory control.~~
- ~~Wireless Sensor Networks: These networks provide wireless process instrumentation networks. Wireless sensor networks are highly secure, typically configured for wireless mesh for robustness, reliability and scalability and are lower data rates than wireless plant networks. These networks provide device interoperability for multi-vendor solutions. Most of wireless instruments are battery operated. These networks are being used in monitoring applications all the way to closed loop, supervisory control.~~

- ~~Proprietary wireless networks: These systems are typically based on single vendors and may take various forms but most often they are used for data transport from remote operations sites.~~

~~Wireless Application Considerations~~

~~**Wireless Plant Network** – these networks should be rigorously planned, designed and configured to provide proper application robustness and throughput. The supplier may perform a site survey to determine the best installation location(s) for the access point(s) and other possible RF sources within the facility. Security should also be taken into account during the design and implementation. Methods such as WPA2 and RADIUS should be implemented to ensure proper authentication, authorization and accounting. Consideration should also be given to how these networks are integrated into the overall plant network. Proper protection such as firewalls should be designed into the solution.~~

~~**Wireless Sensor Network** – these networks should be planned, designed and configured to ensure high reliability and robustness. The supplier may have network design tools and system design and integration guidelines to facilitate the planning and design process. Network capacity in the form of number of devices and overall data throughput must be considered. System integration for the process data and diagnostics must be planned to ensure the instrument value is realized.~~
~~In general the facility should develop an overall RF management plan to document the RF spectrum usage in and around the facility.~~

~~Performance Monitoring and KPI's~~

~~**Wireless Plant Network** – these networks may use standard monitoring mechanisms such as SNMP and/or vendor specific monitoring software.~~

~~**Wireless Sensor Networks** – A wireless user may ask a supplier which high level key process indicators are provided to help them ensure the network is operating reliably. These KPI's may include parameters such as data reliability, average latency and receive signal strength. These parameters may be available for each device in the network.~~