Process Instrumentation and Control

API RECOMMENDED PRACTICE 554
FIRST EDITION, SEPTEMBER 1995

American Petroleum Institute
1220 L Street, Northwest
Washington, D.C. 20005



COPYRIGHT 2002; American Petroleum Institute

Document provided by IHS Licensee=Sincor Venezuela/5934214100, User=, 08/13/2002 12:13:45 MDT Questions or comments about this message: please call the Document Policy Management Group at 1-800-451-1584.

Process Instrumentation and Control

Manufacturing, Distributing, and Marketing

API RECOMMENDED PRACTICE 554
FIRST EDITION, SEPTEMBER 1995

American
Petroleum
Institute



COPYRIGHT 2002; American Petroleum Institute

Document provided by IHS Licensee=Sincor Venezuela/5934214100, User=,
08/13/2002 12:13:45 MDT Questions or comments about this message: please call
the Document Policy Management Group at 1-800-451-1584.

SPECIAL NOTES

1. API PUBLICATIONS NECESSARILY ADDRESS PROBLEMS OF A GENERAL NATURE. WITH RESPECT TO PARTICULAR CIRCUMSTANCES, LOCAL, STATE, AND FEDERAL LAWS AND REGULATIONS SHOULD BE REVIEWED.

2. API IS NOT UNDERTAKING TO MEET THE DUTIES OF EMPLOYERS, MANUFACTURERS, OR SUPPLIERS TO WARN AND PROPERLY TRAIN AND EQUIP THEIR EMPLOYEES, AND OTHERS EXPOSED, CONCERNING HEALTH AND SAFETY RISKS AND PRECAUTIONS, NOR UNDERTAKING THEIR OBLIGATIONS UNDER LOCAL, STATE, OR FEDERAL LAWS.

3. INFORMATION CONCERNING SAFETY AND HEALTH RISKS AND PROPER PRECAUTIONS WITH RESPECT TO PARTICULAR MATERIALS AND CONDITIONS SHOULD BE OBTAINED FROM THE EMPLOYER, THE MANUFACTURER OR SUPPLIER OF THAT MATERIAL, OR THE MATERIAL SAFETY DATA SHEET.

4. 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.

5. GENERALLY, API STANDARDS ARE REVIEWED AND REVISED, REAFFIRMED, OR WITHDRAWN AT LEAST EVERY FIVE YEARS. SOMETIMES A ONE-TIME EXTENSION OF UP TO TWO YEARS WILL BE ADDED TO THIS REVIEW CYCLE. THIS PUBLICATION WILL NO LONGER BE IN EFFECT FIVE YEARS AFTER ITS PUBLICATION DATE AS AN OPERATIVE API STANDARD OR, WHERE AN EXTENSION HAS BEEN GRANTED, UPON REPUBLICATION. THE STATUS OF THE PUBLICATION CAN BE ASCERTAINED FROM THE API AUTHORING 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.

Copyright © 1995 American Petroleum Institute

COPYRIGHT 2002; American Petroleum Institute

Document provided by IHS Licensee=Sincor Venezuela/5934214100, User=, 08/13/2002 12:13:45 MDT Questions or comments about this message: please call the Document Policy Management Group at 1-800-451-1584.

FOREWORD

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

Suggested revisions are invited and should be submitted to the director of the Manufacturing, Distribution, and Marketing Department, American Petroleum Institute, 1220 L Street, N.W., Washington, D.C., 20005.

COPYRIGHT 2002; American Petroleum Institute

Document provided by IHS Licensee=Sincor Venezuela/5934214100, User=, 08/13/2002 12:13:45 MDT Questions or comments about this message: please call the Document Policy Management Group at 1-800-451-1584.

CONTENTS

Page

SECTION 1—PROCESS INSTRUMENTATION AND CONTROL OVERVIEW

1.1 Introduction 1
1.2 Scope 1
1.2.1 Section 2—Scope 1
1.2.2 Section 3—Scope 1
1.2.3 Section 4—Scope 1
1.2.4 Section 5—Scope 1
1.3 Organization of the Recommended Practice 1
1.4 Referenced Publications 1
1.5 Definitions 3
1.5.1 Glossary of Terms 3
1.5.2 Attributes 4
1.5.3 Acronyms 4

SECTION 2—AUTOMATIC CONTROL SYSTEMS

2.1 General 5
2.1.1 Introduction 5
2.1.2 Scope 5
2.1.3 Referenced Publications 5
2.2 Single-Loop Controllers 5
2.2.1 Definition/Scope 5
2.2.2 Types of Single-Loop Controllers 5
2.2.3 Location 5
2.2.4 Site Preparation 5
2.3 Multiloop Controllers 6
2.3.1 Definition/Scope 6
2.3.2 Location and Site Preparation 6
2.4 Programmable Logic Controllers 7
2.4.1 Definition 7
2.4.2 Program Development 7
2.4.3 Operator Interface 7
2.4.4 Diagnostics 7
2.4.5 System Hardware 7
2.5 Distributed Control System 9
2.5.1 General 9
2.5.2 Design Considerations 9
2.5.3 Operator Interface 11
2.5.4 Data Historization 13
2.5.5 Control Functions 13
2.5.6 Configuration and Programming 14
2.5.7 Foreign Device Interface 14
2.5.8 Communications 15
2.5.9 System Performance 15
2.6 Testing 15
2.6.1 Manufacturing Testing 15
2.6.2 System Staging and Integration 16
2.6.3 Factory Acceptance Testing 16
2.6.4 Site Acceptance Test and Operability Evaluation 16

COPYRIGHT 2002; American Petroleum Institute

Document provided by IHS Licensee=Sincor Venezuela/5934214100, User=, 08/13/2002 12:13:45 MDT Questions or comments about this message: please call the Document Policy Management Group at 1-800-451-1584.

Page

2.7 Documentation 17

SECTION 3—ALARMS AND PROTECTIVE DEVICES

3.1 Scope 18
3.2 Referenced Publications 18
3.3 General 18
3.4 Alarm Systems 18
3.4.1 Dedicated Alarm Systems 18
3.4.2 Integrated Alarm Systems 19
3.4.3 Method of Operation 20
3.4.4 Audible Indication 21
3.4.5 Testing 21
3.4.6 Safety Considerations 21
3.4.7 Documentation 21
3.5 Protective Systems 21
3.5.1 Types of Protective Systems 22
3.5.2 Sensor Considerations 22
3.5.3 Shutdown Alarms 23
3.5.4 Preshutdown Alarms 23
3.5.5 Final Control Elements 23
3.5.6 Logic 23
3.5.7 Testing 24
3.5.8 Enhancing Reliability of Protective Systems 24
3.5.9 Documentation 24
3.6 Engineering Considerations 24
3.6.1 General Requirements 24
3.6.2 Electrical Requirements 25
3.6.3 Installation 25

SECTION 4—PROCESS CONTROL COMPUTING ENVIRONMENT

4.1 Scope 26
4.2 Referenced Publications 26
4.3 Plant Computer and Network Architecture 26
4.4 Process Control Computer Functions 26
4.5 Performance Requirements 26
4.5.1 Performance of the Process Control Computing Environment 26
4.5.2 Control Information Processing 27
4.5.3 Display Response 27
4.5.4 Data Acquisition 28
4.5.5 Connectivity Between Plant Networks 28
4.5.6 Potential Limitations in the Architecture 28
4.6 Network Requirements 28
4.6.1 Network Architecture 28
4.6.2 Network Protocols 30
4.7 Hardware Requirements 30
4.7.1 General Design Considerations 30
4.7.2 Central Processing Unit 31
4.7.3 Main Memory 31
4.7.4 System Clock 31
4.7.5 Bulk Storage Devices 31
4.8 Peripherals 32
4.8.1 System Terminal 32

COPYRIGHT 2002; American Petroleum Institute

Document provided by IHS Licensee=Sincor Venezuela/5934214100, User=, 08/13/2002 12:13:45 MDT Questions or comments about this message: please call the Document Policy Management Group at 1-800-451-1584.

Page

4.8.2 Operator Station 32
4.8.3 Engineering Stations 32
4.8.4 Printers 32
4.9 Non-Network Communications Ports 32
4.10 Software Requirements 32
4.10.1 Organization of Process Computer Software 32
4.10.2 Operating System 33
4.10.3 PCC Applications and Interfaces 33
4.10.4 Data Management and the Global Database 38
4.11 Human Interfacing 40
4.11.1 Introduction 40
4.11.2 User Groups in the Process Computing Environment 40
4.11.3 User Requirements 41
4.12 Connection to Other Environments 42
4.12.1 Connection to Higher-Level Computers 42
4.12.2 Connection to Peer Systems 42
4.12.3 Subsystem Communications 42
4.13 Software Reliability 42
4.14 Application Programming 42
4.14.1 Custom Versus Packaged Application Software 43
4.14.2 Application Error Message 43
4.15 Testing/Development Environment 43
4.16 Installation and Support Requirements 43
4.16.1 Installation 43
4.16.2 Support 44

SECTION 5—CONTROL CENTERS

5.1 General 46
5.1.1 Scope 46
5.1.2 Referenced Publications 46
5.1.3 General Considerations 46
5.2 Control Center Design Considerations 47
5.2.1 Size 47
5.2.2 Safety 47
5.3 Control Center Interior Design 48
5.3.1 General 48
5.3.2 Control Room 48
5.3.3 Auxiliary Equipment and Utilities 48
5.3.4 Lighting 49
5.3.5 Ceiling 50
5.3.6 Floor Design 50
5.3.7 Painting 50
5.3.8 Static Electricity 50
5.4 Internal Environment 50
5.4.1 General 50
5.4.2 Heating, Ventilating, and Air-Conditioning 51
5.4.3 Air Purification 51
5.4.4 Positive Air Pressure Systems 51
5.4.5 Fresh Air Intake 52
5.4.6 Noise 52
5.4.7 Hazardous Vapor 52
5.4.8 Fire Protection 52

COPYRIGHT 2002; American Petroleum Institute
Document provided by IHS Licensee=Sincor Venezuela/5934214100, User=, 08/13/2002 12:13:45 MDT Questions or comments about this message: please call the Document Policy Management Group at 1-800-451-1584.

Page

5.4.9 Electrical Grounding 53
5.4.10 Electromagnetic Interference 53
5.5 Satellite Instrument Houses 53
5.5.1 General 53
5.5.2 Location 53
5.5.3 Construction 53
5.5.4 HVAC System 53
5.5.5 Auxiliary Equipment 54
5.5.6 Power Distribution and Wiring 54
5.5.7 Lighting 54
5.5.8 Internal Layout 54
5.6 Control Consoles and Panels 54
5.6.1 General 54
5.6.2 Console Styles 54
5.6.3 Space Considerations 54
5.6.4 DCS/CRT Installation Considerations 54
5.6.5 Panel Styles 55
5.6.6 Instrument Arrangements 55
5.6.7 Space Considerations 57
5.6.8 Fabrication 57
5.6.9 Electrical Considerations 57
5.6.10 Instrument Air Piping 58
5.6.11 Instrument Tubing 59

Figures

1—Functional Process Instrumentation, Control, and Information Network Architecture, View A 2
2—Schematic Showing Dedicated Alarm System 19
3—Schematic Showing Integrated Distributed Control System Alarm and Safety Shutdown System 19
4—Typical Protective System With On-line Testing Capabilities 22
5—Typical Protective System With Testing Feature 23
6—Functional Process Instrumentation, Control, and Information Network Architecture, View B 29
7—PCC Memory Layout 34
8—PCC Device Drivers 35
9—PCC Data Acquisition and History 36
10—PCC Process Control Applications 37
11—PCC User Software 38
12—Example of a Record 39
13—Typical Console 55
14—Typical Panel Shapes 56
15—Typical Field Panels 57

Tables

1—Time Period for System Functions 15
2—Typical Alarm Operating Sequence 21
3—Major Types of Protocols and Media 30
4—In-Service Lighting Requirements 50

COPYRIGHT 2002; American Petroleum Institute

Document provided by IHS Licensee=Sincor Venezuela/5934214100, User=, 08/13/2002 12:13:45 MDT Questions or comments about this message: please call the Document Policy Management Group at 1-800-451-1584.

Process Instrumentation and Control

SECTION 1—PROCESS INSTRUMENTATION AND CONTROL OVERVIEW

1.1 Introduction

This recommended practice (RP 554) covers the performance requirements and considerations for the selection, specification, installation, and testing of process instrumentation and control systems. Control centers as used in the petroleum industry are also covered.

This practice is not intended to be used as a purchase specification, but makes recommendations for minimum requirements and can be used to provide guidance for the development of detailed designs and specifications.

1.2 Scope

1.2.1 SECTION 2—SCOPE

Section 2 of RP 554 provides considerations for the selection, specification, and installation of automatic control systems for use in refinery processes. Single-loop controllers, multiloop controllers, programmable controllers, and distributed control systems are discussed with relevant design and application engineering information.

1.2.2 SECTION 3—SCOPE

Section 3 recommends systems, installation considerations, and testing procedures for alarms and protective devices used in refineries.

1.2.3 SECTION 4—SCOPE

Section 4 of this document covers the performance requirements, networks, hardware, software, and infrastructure associated with the process control computing environment. The intent of this recommended practice is to provide guidance to those parties developing detailed specifications for computing resources used for process control and associated functions in the petroleum industry. This document is based on the philosophy of using widely accepted computing industry standards and avoiding custom or proprietary approaches.

This document does not cover the application software requirements associated with process control, advanced control, process optimization, and data acquisition.

1.2.4 SECTION 5—SCOPE

Section 5 presents recommended practices for the design and installation of control centers for processing operations. Recommended practices for blast-resistant control centers design is not within the scope of this document.

1.3 Organization of the Recommended Practice

Following a glossary of terms, acronyms list and an overall functional architecture figure (see Figure 1), this recommended practice is divided into four distinct and independent sections covering the following topics:

a. Section 2—Automatic Control Systems:
   1. Single-loop controllers.
   2. Multiloop controllers.
   3. Programmable logic controllers (PLCs).
   4. Distributed control systems (DCSs).
   5. Testing of automated control systems.

b. Section 3—Alarm and Protective Devices:
   1. Alarm systems.
   2. Protective systems.
   3. General requirements for alarm.
   4. Protective systems.

c. Section 4—Process Control Computing Environment:
   1. Performance requirements.
   2. Network requirements.
   3. Hardware requirements.
   4. Software requirements.
   5. Infrastructure requirements.

d. Section 5—Control Centers:
   1. Control center design considerations.
   2. Control center interior design.
   3. Internal environment.
   4. Satellite instrument houses.
   5. Control consoles and panels.

Figure 1 is a composite functional overview of several options that may be found in a process instrumentation and control environment. The areas covered by the various sections of this recommended practice are outlined to guide the user to the appropriate section. The architecture depicts several levels of instrument and control functions, with each lower level in the hierarchy responsible for a narrower and more specific control function. This architecture is not intended to endorse or limit any specific hardware or software solution, but rather shows hardware and network variations that are discussed in the appropriate sections.

1.4 Referenced Publications

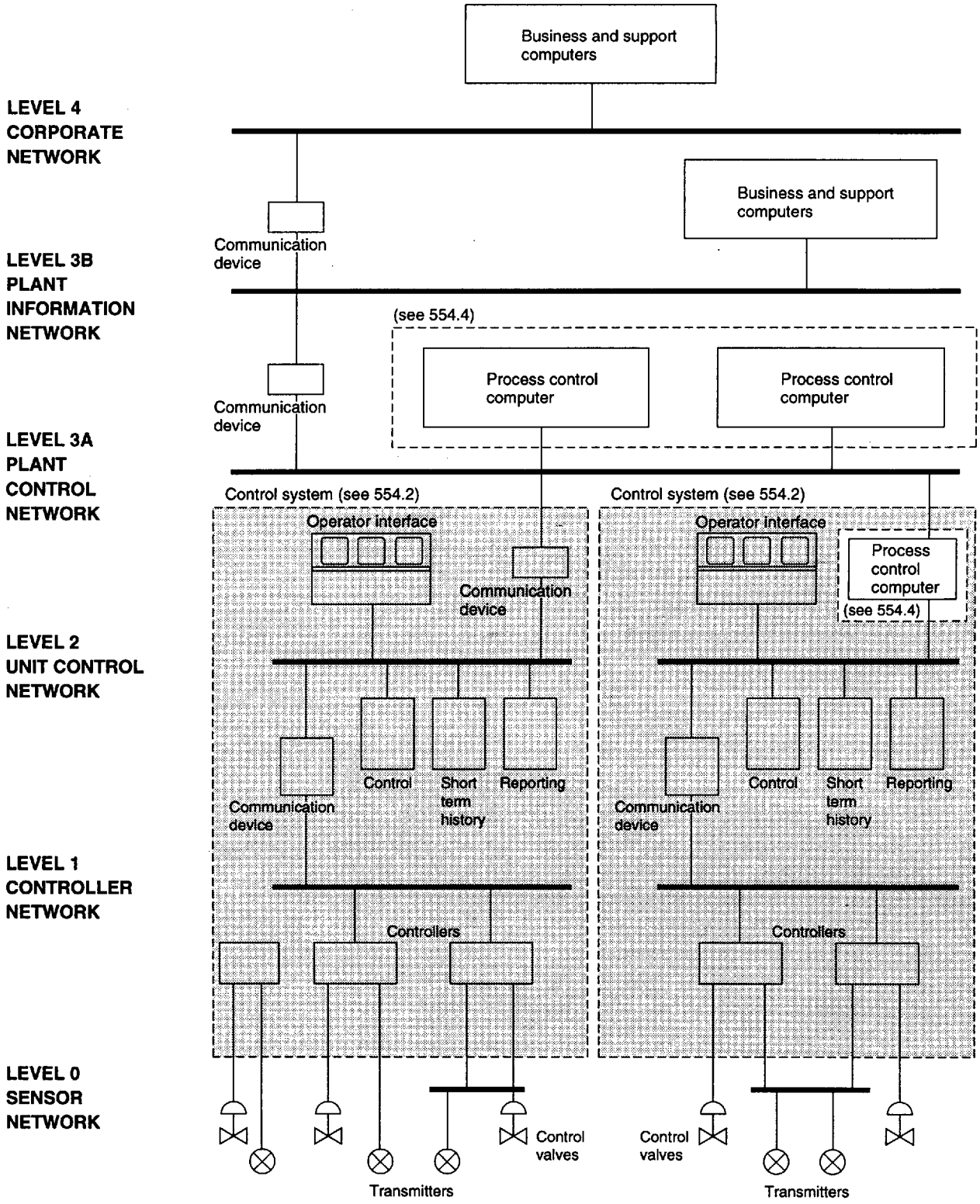
The latest revision of the following publications are cited in this recommended practice.

ANSI[1]

[1]American National Standards Institute, 11 West 42nd Street, New York, NY 10036.

COPYRIGHT 2002; American Petroleum Institute

Document provided by IHS Licensee=Sincor Venezuela/5934214100, User=, 08/13/2002 12:13:45 MDT Questions or comments about this message: please call the Document Policy Management Group at 1-800-451-1584.



Note: 554.2 is equivalent to Section 2 of this RP and
554.4 is equivalent to Section 4 of this RP.

Figure 1—Functional Process Instrumentation, Control, and Information Network Architecture, View A

COPYRIGHT 2002; American Petroleum Institute

Document provided by IHS Licensee=Sincor Venezuela/5934214100, User=,
08/13/2002 12:13:45 MDT Questions or comments about this message: please call
the Document Policy Management Group at 1-800-451-1584.

Z97.1 *Safety Glass*

API

RP 500 *Classification of Locations for Electrical Installations at Petroleum Facilities*
RP 540 *Electrical Installations in Petroleum Processing Plants*
RP 551 *Process Measurement and Instrumentation*
RP 552 *Transmission Systems*
RP 556 *Fired Heaters and Steam Generators*, expected publication date of 1996.
Std 612 *Special-Purpose Steam Turbines for Refinery Services*
Std 614 *Lubrication, Shaft-Sealing, and Control-Oil Systems for Special Purpose Applications*
Std 616 *Gas Turbines for Refinery Services*
Std 617 *Centrifugal Compressors for General Refinery Service*
Std 618 *Reciprocating Compressors for General Refinery Service*
Std 619 *Rotary-Type Positive Displacement Compressors for General Refinery Service*
Std 674 *Positive Displacement Pumps-Reciprocating*
Std 675 *Positive Displacement Pumps-Controlled Volume*
Std 676 *Positive Displacement Pumps-Rotary*
RP 750 *Management of Process Hazards*

ARI[2]

Std 210-240-89 *Unitary Air-Conditioning and Air Source Heat Pump Equipment*

ASHRAE[3]

Handbook (four volumes)

Standard Safety Code 15 for Mechanical Refrigeration

FIPS[4]

Guideline on Electrical Power for ADP Installations-FIPS PUB 4

IEEE[5]

610-12 *AAA Recommended Practice for Emergency and Stand By Power Systems for Individual and Commercial Applications*
446 *Recommended Practice for Emergency and Standby Power Systems for Industrial and Commercial Applications*
484 *Practice for Installation Design and Installation of Large Lead Storage Batteries for Generating Stations and Substations*

ISA[6]

S5.5 *Process Instrumentation Terminology*
RP12.4 *Instructions for Purging for the Reduction of Hazardous Area Classifications*
SP18.1 *Annunciator Sequences and Specifications*
RP60.1 *Control Center Facilities*
S71.04 *Environmental Conditions for Process Measurement and Control Systems: Airborne Contaminants*
SP88.01 *Batch Control Systems: Models and Terms*

MCA[7]

SG-22 *Siting and Construction of New Control House for Chemical Manufacturing Plants*

NFPA[8]

70 *National Electric Code*
Article 440 *Air-Conditioning and Refrigeration Equipment*
700-12(a) *Chapter 7 Emergency Systems Sub Section C Sources of Power 700-12 General Requirement (a) Storage Battery*
Article 250 *Grounding*
Article 500 *Hazardous (Classified) Locations*
75 *Standard for the Protection of Electronic Computer/Data Processing Equipment*
493 *Intrinsically Safe Apparatus in Division 1 Hazardous Locations*
496 *Purged and Pressurized Enclosures for Electrical Equipment*
497A *Fire Protection Handbook*

OSHA[9]

29 *Code of Federal Regulations*

UL[10]

779 *Electrically Conducted Floorings*

1.5 Definitions

1.5.1 GLOSSARY OF TERMS

The following are definitions of terms used in this document.

[2]Air-Conditioning and Refrigeration Institute, 4301 North Fairfax Drive, Arlington, VA 22203.
[3]American Society of Heating, Refrigeration, and Air-Conditioning Engineers, 1791 Tullie Circle, N.E., Atlanta, GA 30329.
[4]Federal Information Processing Standards, U.S. Department of Commerce, Quince Orchard and Clopper Roads, Gaithersburg, MD, 20899.
[5]Institute of Electrical and Electronics Engineers, 345 East 47th Street, New York, NY 10017.
[6]Instrument Society of America, P.O. Box 12277, Research Triangle Park, NC 27709.
[7]Chemical Manufacturing Association, 2501 M Street, N.W., Washington, D.C. 20037.
[8]National Fire Protection Association, 1 Batterymarch Park, Quincy, MA 02169-9473.
[9]Occupational Health and Safety Administration, U.S. Department of Labor. The *Code of Federal Regulations* is available from the U.S. Government Printing Office, Washington, D.C. 20402.
[10]Underwriters Laboratories, 333 Pfingsten Road, Northbrook, IL 60062.

COPYRIGHT 2002; American Petroleum Institute

Document provided by IHS Licensee=Sincor Venezuela/5934214100, User=, 08/13/2002 12:13:45 MDT Questions or comments about this message: please call the Document Policy Management Group at 1-800-451-1584.

1.5.1.1 *Process control computing environment* refers to software and controls in the process computer rather than the management computer or distributed control system environment.

1.5.1.2 *Process control computer* refers to a computer whose primary purpose is to control process activities, not business. It is a real-time computer with extensive connections to field instrument inputs and outputs either directly or through data communication links.

1.5.1.3 *Network* refers to a communication path, either twisted pair, coaxial, or fiber-optic. The network becomes the input/output (I/O) path for several distributed network devices along its length.

1.5.1.4 *Corporate network* refers to the high-level business computer network that serves the headquarters group.

1.5.1.5 *Plant information network* refers to the highest-level computer network which serves various plant departments and is not a control network.

1.5.1.6 *Plant control network* refers to the network within a plant that has control functions circulating between various processing locations.

1.5.1.7 *Unit control network* refers to a network which is to control one or more process units.

1.5.1.8 *Controller network* refers to a network with distributed or lumped controllers along its length that can communicate with each other and other distributed devices.

1.5.1.9 *Sensor network* refers to a network which contains sensors along its length such as the projected ISA SP50.

1.5.2 ATTRIBUTES

The following are definitions of attributes.

1.5.2.1 *Fan in* refers to a number of inputs brought together in one place.

1.5.2.2 *Bulk storage* usually refers to a large-volume memory or storage device, disk drive, or tape device.

1.5.2.3 *Control loop* refers to that part of an instrument control system which includes the final control element (control valve, damper, variable speed drive, and so on) and the controlling algorithm which may be PID, digital, and so forth.

1.5.2.4 *Data dictionaries* are a collection of all of the names of the data used in software programs.

1.5.2.5 *Faraday cage* refers to a conducting enclosure that can shield transmission of external and internal electrical fields and radiated energy to it.

1.5.2.6 *Global data* refers to data that can be accessed by two or more non-nested modules of a program without being explicitly passed as parameters between the modules (IEEE 610-12).

1.5.2.7 *Human interfacing* refers to the art of interfacing with the user, usually a keyboard and CRT in this standard.

1.5.2.8 *Interoperability* refers to the ability to operate between different modules of programs or between different pieces of hardware.

1.5.2.9 *Library shared program* refers to a software program issued as part of a larger application library of programs that can be used in different software modules simultaneously.

1.5.2.10 *Loop folder* refers to a folder, electronic, or paper file that contains all of the items in an instrument loop that are required for field checkout and startup during initial construction. This file includes loop drawings, configuration data, witness test signoff sheets, and the like.

1.5.2.11 *Windowing* refers to the ability of software programs to break the CRT into simultaneous or overlapping zones with separate data presentation at the same time.

1.5.3 ACRONYMS

The following are definitions of acronyms used in this document.

1.5.3.1 *CPU* stands for the central processing unit in a computer, contains the master clock.

1.5.3.2 *DCS* stands for a distributed control system; various functions of control are distributed over a network, usually digital.

1.5.3.3 *PCC* stands for process control computer, a real time computer used to process control algorithms on input data and distribute the answers to the appropriate output device in the field.

1.5.3.4 *PLC* stands for a programmable logic controller.

1.5.3.5 *I/O* stands for inputs and outputs.

1.5.3.6 *OSI* stands for open signal interconnection and open systems interconnection.

COPYRIGHT 2002; American Petroleum Institute

Document provided by IHS Licensee=Sincor Venezuela/5934214100, User=, 08/13/2002 12:13:45 MDT Questions or comments about this message: please call the Document Policy Management Group at 1-800-451-1584.

SECTION 2—AUTOMATIC CONTROL SYSTEMS

2.1 General

2.1.1 INTRODUCTION

These guidelines should be considered whenever applying automatic control systems to refinery processes. The engineered configuration will depend on the equipment selected and on the specific needs of the particular application.

Inherent in these recommendations is the assumption that automatic control systems are for continuous control, sequential control, and monitoring of one or more process units operated from one or more central control locations.

2.1.2 SCOPE

This recommended practice provides considerations for the selection, specification, and installation of automatic control systems for use in refinery processes. Single-loop controllers, multiloop controllers, programmable controllers, and distributed control systems are discussed with relevant design and application engineering information.

2.1.3 REFERENCED PUBLICATIONS

The latest editions or revisions of the following publications shall, to the extent specified, form a part of this recommended practice: API RP 552, ANSI/ISA S5.5, ISA SP88.01 (see 1.4 for titles and publication information).

2.2 Single-Loop Controllers

2.2.1 DEFINITION/SCOPE

A single-loop controller is a device dedicated to generating a single control output. This controller incorporates an operator interface consisting of individual displays of the process variable, the setpoint, and the output, as well as the means of adjusting the setpoint, the output, switching to manual operation, or changing ratios. Pneumatic controllers are not separately discussed.

2.2.2 TYPES OF SINGLE-LOOP CONTROLLERS

There are two basic types of single-loop controllers.

a. Direct-connected controllers—These are mechanically, electrically, or hydraulically connected to the measured variable via a pressure element, thermocouple, filled thermal system, or other means. Output from these controllers are commonly pneumatic (3 to 15 pounds per square inch gauge metric units) (20 to 100 kilopascals) or electronic (4 to 20 milliampere direct current).

b. Receiver-type controllers—These receive an input from an external device such as a transmitter. Based on the received signal, the controller can be the following:

1. Pneumatic—The input/output signals are usually 3 to 15 psig (20 to 100 kPa).
2. Analog Electronic—The input/output signals are usually 4 to 20 maDC. Circuitry in the controller is based on analog electronic techniques.
3. Digital Electronic—The input/output signals are usually 4 to 20 maDC while all control functions are in software. Digital controllers are often designed to accept a number and variety of input signals and provide a selection of programming functions to support control strategies. All digital controllers contain a microprocessor and associated memory.

2.2.3 LOCATION

Controllers can be mounted on the control room panels with an integral operator interface, on racks with panel-mounted operator interface, in the field near the point of measurement, or directly on the control valve.

The following points (not listed in order of importance) should be considered when deciding on the location for a single-loop controller:

a. Convenience to operating personnel.
b. Convenience to maintenance personnel, accessibility for servicing, and frequency of servicing.
c. Installed cost, based on location.
d. Safety of personnel and equipment.
e. Vibration effects on equipment and its performance.
f. Corrosion caused by the surrounding atmosphere.
g. Weatherproofing and winterizing.
h. Explosion proofing.
i. Protection from fire.
j. Accessibility in the event of fire.
k. Protection from mechanical damage, or damage caused by fire suppression systems.
l. Ambient temperature.
m. Thermal radiation from the sun or hot equipment.
n. Plant philosophy with respect to types of instruments purchased and their location.
o. Manpower availability.
p. Protection from the effects of EMI (electro magnetic interference) or RFI (radio frequency interference).
q. Reliability/availability of controller power source.

Pneumatic controllers are often mounted locally because there is little justification for control room mounting, and/or transmission lag must be reduced. It is sometimes desirable to have an indicator and/or remotely generated setpoint available in the control room.

2.2.4 SITE PREPARATION

2.2.4.1 Pre-Installation Procedures

Careful consideration of manufacturer's data is required, particularly when connecting various manufacturer's products together. The following factors are especially important:

COPYRIGHT 2002; American Petroleum Institute

Document provided by IHS Licensee=Sincor Venezuela/5934214100, User=, 08/13/2002 12:13:45 MDT Questions or comments about this message: please call the Document Policy Management Group at 1-800-451-1584.

2.2.4.1.1 Maximum and minimum permissible electrical load should be considered (refer to the manufacturer's specifications). This applies to both input and output circuits; the controller often is used to power the transmitter; the minimum voltage available to the transmitter, as well as the load of controller and other input circuit devices (recorder, process variable alarms, computers, and so on), all become considerations. The load capacity of these circuits should be no less than 550 ohms. The signal common to the controller may be referenced to ground in the controller output circuit. Also, verify that only one signal common point of reference exists for the current loop.

2.2.4.1.2 Grounding of electronic controllers, as with most electronic equipment, is critical. Do not ground at more than one point. Refer to API RP 552 and the manufacturer's recommendations for details.

2.2.4.1.3 Signal wiring should be kept separate from power wiring—particularly any wiring subject to voltage surges, such as those resulting from switching of lights, motors, and so forth. When signal wiring and power wiring cross, they should cross at 90 degrees.

2.2.4.1.4 Moisture, conductive dust, or corrosive atmospheres degrade the reliability and performance of electronic instruments. Consult the manufacturer's specifications for exact limits, as well as performance influences.

2.2.4.1.5 If an intrinsically safe (IS) system is specified, consideration must be given to meeting IS requirements and total loop impedance.

2.2.4.1.6 Reliability and distribution of power should be considered.

2.2.4.2 Post-Installation Procedures

a. Perform a critical visual inspection for damage that may have occurred during shipment or installation. Check connections for correctness and obvious irregularities, such as loose piping or tubing fittings, loose wiring, and improperly secured printed circuit boards. Remove all shipping stops, supports, or packing materials.

b. Inspect each instrument item to certify that it conforms to the requisitions and documentation.

c. Determine, particularly on field-mounted controllers, that controllers have been properly mounted in an appropriate location. Inspect the location, considering accessibility for maintenance and operation. Inspect also for correct hazardous area classification and proper environmental protection.

d. Following the manufacturer's instruction manual carefully, check each controller in the following general manner. (Note that, at the inspector's option, these checks may be performed with the controller in place or at a bench calibration location).

1. Set up a record or loop folder for each instrument and record the test results. Worksheet guides for instrument records are available from a number of sources. The format should include the following:
   (a) Tag number.
   (b) Manufacturer, model, serial number.
   (c) Date of acceptance test.
   (d) Controller type, for example, PI, PID, and so forth.
   (e) Condition of instrument, as found.
   (f) Corrective action taken.
   (g) Condition of instrument, as left.
   (h) Calibration data.
   (i) Recommendation for further action or disposition.
   (j) Application description.
2. Apply a suitable source of air and/or electrical power to the appropriate connections.
3. Provide an appropriate variable input signal to simulate the process variable.
4. Connect the output to a suitably scaled electronic test meter or through a capacity chamber to a test gauge.
5. Carry out a complete operational check making necessary adjustments to demonstrate functions such as proper alignment and tracking, control modes (proportional, integral or derivative), direct and reverse action, auto/manual/remote transfer, and calibration.
6. On receiver controllers, an additional *closed loop* checking method may be used. For this test, the controller is set at reverse action. Its output is then connected to its input through a resistance/capacitance network to behave like a fast-acting control loop. All functions of the controller can be checked under these simulated process conditions.
7. Perform a complete loop test prior to start-up, with controller in place. Verify that the correct transmitter is connected to the controller input, and perform a three-point calibration check.

   Use the manual output to stroke the valve or other output device. Check that the controller action (direct or reverse) has been set properly.
8. Set the controller with safe tuning constants for service.

2.3 Multiloop Controllers

2.3.1 DEFINITION/SCOPE

A *multiloop controller* is a stand-alone digital controller capable of accepting two or more process inputs and providing two or more control outputs. A controller microprocessor is shared to perform control functions for two or more loops.

Multiloop controllers can also be used for applications involving loop interaction and logic functions such as those commonly used in distillation column, compressor, or boiler control strategies.

2.3.2 LOCATION AND SITE PREPARATION

Multiloop controllers are installed, using the same guidelines as single-loop controllers.

COPYRIGHT 2002; American Petroleum Institute

Document provided by IHS Licensee=Sincor Venezuela/5934214100, User=, 08/13/2002 12:13:45 MDT Questions or comments about this message: please call the Document Policy Management Group at 1-800-451-1584.

2.4 Programmable Logic Controllers

2.4.1 DEFINITION

A *typical programmable logic controller* (PLC) consists of a programming unit, a processing unit, an I/O unit, and a power supply.

Programmable logic controllers are microprocessor-based solid state devices which are programmed to operate in a particular sequence in response to external inputs. PLCs can be used in place of relay systems or for proportional, integral, and derivative (PID) control in specific applications.

The programming techniques commonly used to express sequential on-off logic include ladder diagrams or boolean logic. Programmable controller logic resides in a memory, which can be modified to allow for changes in the applications or to correct errors in the initial programming.

2.4.2 PROGRAM DEVELOPMENT

2.4.2.1 Programming Devices

A *programming device* is a dedicated device that allows an interface to the PLC for program development, start-up, and troubleshooting. The instructions to be executed by the PLC are inserted into its memory with this device. Programmer devices vary in size from small handheld units to CRT-based units with engineering development documentation, I/O status, and on-line/off-line programming.

2.4.2.2 Programming Terminals

With appropriate software, programming may be done off-line on a personal computer.

A programming terminal should be used for program development, program storage, fault diagnostics, system monitoring, and application documentation. Software and hardware shall record the user-defined logic programming on a removable disk media for security and backup.

Programming terminal should allow manual forcing of input or output states and provide the resulting status on ladder logic displays and/or printouts in on-line and/or off-line modes.

All programming should be done using alphanumeric tagname references and should allow on-screen comments for a functional description of an application program.

The programming terminal may provide a display of all system diagnostic states.

Off-line programming may provide run emulation capability for testing and troubleshooting of the application program. Software changes should be done off-line, tested, and then downloaded into the running application.

2.4.2.3 Program Protection

The program should be protected from unauthorized changes by the use of security measures such as passwords or key lock switches. To protect against inadvertent changes in the programs, the approved version should be stored in a limited-access environment for change control and possible fast restoration.

2.4.3 OPERATOR INTERFACE

2.4.3.1 Some PLCs are equipped with CRTs that can give the operator access to data, such as timers, counters, loops, operational displays and the like but not access to the program itself.

2.4.3.2 Push-button/indicator light panels or a CRT display can be installed in field locations for the convenience of field personnel who require some local controls.

2.4.4 DIAGNOSTICS

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

2.4.4.2 PLC on-line diagnostics should do the following:

a. Test all spare boards in the system.
b. Test board ID and status at a minimum frequency of once per minute.
c. Check the I/O board configuration and set the main chassis alarm if boards are missing or faulted.
d. Check I/O boards for faults, including fuse failures where applicable, and if detected, turn on fault LEDS on the board.
e. Perform diagnostics on the communication processor and cables which handle I/O board communication.

2.4.4.3 The PLC must perform diagnostics on its main processor as follows:

a. Diagnostics on the processor and the floating point unit are performed continuously in the background.
b. Random Access Memory (RAM) diagnostics are also performed continuously.
c. The microprocessors on the main processor board are checked for proper response every minute.
d. The control program checksum is verified.
e. Universal Asynchronous Receiver Transmitter (UART) diagnostics are run continuously.
f. The checksum of all program read-only memories (ROMs) on the main processor are checked continuously.
g. Redundant processor and programs are verified as good and current.
h. The PLC should perform extensive power-up diagnostics on the main processor.

2.4.5 SYSTEM HARDWARE

2.4.5.1 Processor

The processor should be modular and removable for maintenance, and electrically isolated from associated I/O components.

COPYRIGHT 2002; American Petroleum Institute

Document provided by IHS Licensee=Sincor Venezuela/5934214100, User=, 08/13/2002 12:13:45 MDT Questions or comments about this message: please call the Document Policy Management Group at 1-800-451-1584.

In the event of power loss, the processor should retain its memory for a minimum of six months.

A real-time clock with a minimum 10 millisecond resolution should be provided for time tagging events, rate calculations, and other time dependent functions.

The processor should be capable of scanning and updating the I/O and of executing user-defined discrete logic a minimum of ten times per second and analog functions a minimum of four times per second.

When combining discrete and analog functions in one processor, the analog functions increase the net processor execution time and should be taken into consideration.

The processor should be able to execute commands using the following functions and parameters:

a. Math functionality using both integer and real numbers.
b. Logic including transitional inputs and latching outputs.
c. Time delays, counters, and timers.
d. Arithmetic, algebraic, and trigonometric functions.
e. PID and process control functions.
f. If-then-else statement programming.
g. Median select and median deviation function for analog input voting.

2.4.5.2 I/O Modules

The input/output components should be self-contained independent modules so that a failure and subsequent replacement of one does not affect other components. All output modules should be replaceable with the I/O system powered.

Modules should have mechanical keying to prevent physical insertion and on-line activation of a module in an incorrect slot in the chassis.

Shorting or grounding the field wires connected to any I/O module shall not damage the module itself.

2.4.5.3 Analog Input Modules

Analog input modules should employ at least 12-bit precision A to D converters for 4 to 20-mA and 1 to 5-volt signals from 2-wire and 4-wire transmitters. Reference junction compensation and linearization must be provided for thermocouple inputs. Input measurement accuracy shall be at least 0.10 percent of range for all inputs. Common mode noise rejection should be at least 80 db. Normal mode noise rejection should be at least 45 db.

Analog inputs should offer signal filtering and be fused or protected from inadvertent grounds.

2.4.5.4 Analog Output Modules

Analog outputs should provide a 4–20 mADC signal and should be capable of operating loops up to 550 ohms resistance minimum. Analog output accuracy shall be at least 0.5 percent.

2.4.5.5 Discrete Input Modules

Each discrete input should have a light-emitting diode (LED) indicator showing input status on the module. Discrete input signals should be conditioned by a low-pass filter, to reduce the effects of noise and bounce. A minimum of 600 VDC opto-isolation should be provided between each input signal and microprocessor.

Discrete inputs should have an input resistance of 20 megohm minimum.

Each discrete input should be individually fused with blown fuse indication.

Frequency (pulse) inputs should have an input resistance of 1 megohm minimum and be capable of handling high-speed pulses of up to 50,000 Hertz.

2.4.5.6 Discrete Output Modules

Each discrete output should have an LED indicator showing output status on the module.

Discrete output modules should provide a minimum of 600 VDC opto-isolation between each output signal and processor.

Each digital output should be individually fused with blown fuse indication. Outputs should not be powered with PLC internal power supply.

2.4.5.7 DCS Interface Module

The PLC should be capable of interfacing to a Distributed Control System (DCS). The information to be transferred to and from the DCS via this interface should include, but is not limited to, the following:

a. Systems alarms and status.
b. Discrete I/O status.
c. Analog I/O values.

The speed of transmission should be such that any change in I/O which is to update on the DCS CRT shall not exceed 4 seconds from time of event to Cathode Ray Terminal (CRT) update.

2.4.5.8 Power Supplies

Power supplies should be redundant for critical PLC applications, with each capable of supplying complete system power. The system should accept power from two different power sources, one of which can be an uninterruptable power supply (UPS). Power supplies may be replaceable on-line without disrupting the process and without impacting PLC control capability.

System power supplies should have over-temperature protection, integral fuse protection, and status LEDs to indicate power supply faults. In addition, each power supply should have an alarm contact to indicate the presence of a fault.

COPYRIGHT 2002; American Petroleum Institute

Document provided by IHS Licensee=Sincor Venezuela/5934214100, User=, 08/13/2002 12:13:45 MDT Questions or comments about this message: please call the Document Policy Management Group at 1-800-451-1584.

2.4.5.9 Spare and Expansion Capacity

At least 20 percent spare capacity should be available within each system. This includes marshalling cabinets, terminations, monitor switches, and I/O. User program memory should have at least 40 percent spare capacity.

At least 20 percent spare space should be available within each system. This includes space in systems and marshalling cabinets for terminations, I/O, and so forth. This 20 percent spare space is in addition to installed spare capacity required.

2.4.5.10 Remote I/O Network

The network shall be secure and capable of communicating to I/O modules over twisted pair, fiber optics, or coax cable of distances of a least 1000 feet.

2.5 Distributed Control System

2.5.1 GENERAL

A Distributed Control System (DCS) is a microprocessor-based control and data acquisition system, comprising multiple modules operating over a network. The system functions can be geographically and functionally distributed. Operator interface to the process is through a console with CRT displays and keyboards. The functions typically available in DCSs are the following:

a. PID control.
b. Discrete control.
c. Advanced control capability.
d. Alarm management.
e. Graphical and schematic displays.
f. Trending of real time and historical data.
g. Communications with other devices and subsystems.
h. Data acquisition.
i. Report generation.
j. Data historization.

2.5.2 DESIGN CONSIDERATIONS

2.5.2.1 Emergency shutdown systems should operate independent of the DCS. However, information may flow from the emergency shutdown system to the DCS for monitoring purposes.

2.5.2.2 DCSs which control more than one major process unit should be located in a secure location. This could be a blast-resistant building or a remote location if the processes are rated hazardous.

2.5.2.3 Although interacting loops may be scattered throughout a system, good practice is to group loops within the same functional area within the same control device.

2.5.2.4 Steps should be taken to evaluate the level of corrosion due to the environment for all locations where DCS components will be installed and to minimize the corrosive effects. This may require some form of monitoring system to ensure that corrosive levels are within acceptable limits. Refer to Section 5.

2.5.2.5 It is recommended to have as much control (including signal conditioning) in the lowest secure level of the control system as practical.

2.5.2.6 Each DCS device connected to the DCS power bus should have individual fuses. Power supplies should be designed for fully loaded cabinets with 20 percent reserve above inrush current.

2.5.2.7 All vendor software and hardware upgrades or fixes must be designed to be done while the system is on-line and backup devices or I/O are operational. After changes of primary devices are complete, the backup devices may be modified.

2.5.2.8 Redundancy

2.5.2.8.1 General

All components that can affect more than two control loops should be redundant such that a single failure does not affect more than two loops nor the loss of any critical operating display. This normally includes control loops, high priority alarms, digital outputs that are in critical service, and CRTs. The data highway should generally be fully redundant with separate routing to avoid a single accident/event from damaging both cables.

2.5.2.8.2 *Redundancy of communication:* The communication system should be fully redundant and both the primary and backup portions should always operate at full speed. No separate transfer mechanism or operator action should be required in the event of a failure. The design should be such that no single point of failure can cause more than one device to be unable to communicate to the rest of the network.

2.5.2.8.3 *Multiloop control unit redundancy:* Controller units should be fully redundant with automatic transfer on failure. The backup unit should maintain a copy of the database of the primary at all times. No transfer of database should occur after a failure is detected. No operator action should be required to implement transfer to the backup unit. Controller units should be stand alone (in other words, if there is a break in communication on the data highway or power failure somewhere else in the system, the controller would continue to function).

2.5.2.8.4 *Input/output module redundancy:* Input/output modules where two or more loops are processed for control and critical functions should be redundant. Certain low priority input only modules need not be redundant.

2.5.2.8.5 *Instrument power supply system:* The DCS should have redundant power supplies. Power supply switching must be automatic from the main supply to the backup supply and must provide an alarm. Loss of any

COPYRIGHT 2002; American Petroleum Institute

Document provided by IHS Licensee=Sincor Venezuela/5934214100, User=, 08/13/2002 12:13:45 MDT Questions or comments about this message: please call the Document Policy Management Group at 1-800-451-1584.

component of the main power supply should not degrade the backup power which must be capable of supplying 100 percent of load. The power supplies should have separate input terminals and breakers in order to connect to two independent sources of incoming AC power.

2.5.2.9 System Expansion

2.5.2.9.1 *Spares and expansion capacity:* A DCS system should be designed for the point count plus 30 percent to allow adequate hardware for job development. This should allow at least 10 percent installed spare capacity at the time of shipment. In order to allow for contingencies, additional advanced control, and future additions, the control system shall be designed for at least a 30 percent physical and processor expansion capacity in each of the following areas:

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

2.5.2.9.3 *Displays:* Expansion of the number displays (blocks, configuration, logic steps, faceplates, graphic trends, and so on) should be without the addition of any hardware or software.

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

2.5.2.9.5 *Commissioning:* The system should allow devices to be added on-line without interruption of control or display, and without degradation of security.

2.5.2.9.6 *Power supplies:* Power supplies should be sized or be modularly expandable to accommodate all anticipated expansion.

2.5.2.10 Security

2.5.2.10.1 *System security:* The DCS must allow operating personnel to quickly, efficiently, securely, and safely monitor and control the process.

As a minimum, it should be possible to initialize all control functions in the manual mode with the function's output set to the actual hardware output. In addition, the control system may provide other configurable types of initialization.

Certain functions and parameters should be designated as *protected* in order to prevent unauthorized activity or changes. They should use keylock, special keyboard, or password features.

2.5.2.10.2 *Security priority levels:* Access to the system should be protected on a priority basis. The access protection shall be either by keylock or a programmable password. Typical priority levels are as follows:

a. Priority 4—View Only: This is the lowest priority and will allow access to all permitted displays in the system but will inhibit the ability to change anything.
b. Priority 3—Operating: With this priority, the operator will have access to all permitted operating displays, trends, alarm displays and alarm acknowledgment, control, setpoints, auto and manual settings, and any other functions (in other words, sequencing) programmed as an operator function.
c. Priority 2—Supervisory/Maintenance: This priority will allow access to all functions of the operating mode as well as access to change alarm setpoints, loop ranges, tuning parameters, and system management functions.
d. Priority 1—Engineering: This is the highest priority and allows access to the entire database and programming, including the security system. There should be an option for restricting changes to outputs or setpoints when in this mode.

The security system should not interfere with normal operator tasks.

2.5.2.11 Reliability

No more than 1 control loop or output device should fail to operate as specified in any continuous 12-month period for each group of 100 control loops and 2 out of 100 for non-control points.

The system should have on-line diagnostic programs for self-checking and security checking/correction so that the primary system and the backup system are periodically checked. It should also be able to disconnect the faulty component, or transfer to backup. The system should have a system status display and should also identify the source of any malfunction.

2.5.2.12 Power Supply

Care must be taken in the design of the power source to the DCS to avoid a single point of failure causing loss of control.

The DCS should be provided with power for continuous operation. Generally one or more uninterruptable power supply (UPS) systems are provided and are supplied from a reliable source of power with an automatic transfer to a backup system. This could be an emergency generator or an alternate source. The nonlinear characteristics of the DCS loads which can produce large harmonic distortions should be considered in the design of the UPS.

These power sources should supply only the control and monitoring systems such as DCS equipment, instrument systems, alarm systems, emergency lighting at the consoles, and the operators radio equipment. All other equipment or systems should be powered from separate sources.

COPYRIGHT 2002; American Petroleum Institute

Document provided by IHS Licensee=Sincor Venezuela/5934214100, User=, 08/13/2002 12:13:45 MDT Questions or comments about this message: please call the Document Policy Management Group at 1-800-451-1584.

2.5.3 OPERATOR INTERFACE

2.5.3.1 Operator Consoles

2.5.3.1.1 Operator stations provide the primary means of operating the process and conveying the operators commands to the control system. The consoles are windows into the control actions performed by the controller units via the communication system.

2.5.3.1.2 Operator consoles should be redundant and include fully independent operator stations, each composed of CRTs, keyboards, and pointing devices with all associated electronics.

2.5.3.1.3 Each console may monitor any section of the plant, but manipulation of any control loop should be limited to only one console at a time. Control access from other consoles should be selectively inhibited by configuration, password, or key lock.

2.5.3.1.4 Each operator station should have identical capability and be interchangeable for all functions, including interactive graphics.

2.5.3.1.5 A back-up operator station located in a remote-control room is not recommended for control, due to the possibility of conflicting operator actions. Such a station should be used for monitoring only.

2.5.3.1.6 No single failure should cause the loss of functionality of the system to less than two CRTs and keyboards. When additional CRTs and keyboards share electronics, there should not be a degradation of the performance of that operator station.

2.5.3.1.7 Operator keyboards and pointing devices should be specifically designed for process control functions. General purpose computer keyboards are normally not acceptable. The keyboards should be reasonably resistant to spills of coffee and other common liquids.

2.5.3.1.8 Dedicated function keys should support the following as a minimum:

a. Cursor control.
b. Display function selection.
c. Alarm functions.
d. Print functions.
e. Trending functions.
f. Control actions.
g. Process point selection.
h. Paging.
i. Data entry.

2.5.3.1.9 The CRT display should have usable resolution of as high as currently available. The display should provide many colors, in both the foreground and background.

2.5.3.1.10 Hard copy devices, printers, or other peripheral devices must not degrade console performance.

2.5.3.1.11 Ergonomic considerations should be taken into account in the design and layout of the operator console. Items to consider should include the room arrangement, lighting, climate, air purity, and sound levels.

2.5.3.2 Engineer's Workstation

2.5.3.2.1 The engineer's workstation should be located in the engineer's area of the main control room and should be interfaced to the DCS.

2.5.3.2.2 The engineer's workstation should be comprised of electronics, storage media, color CRT, engineering keyboard, and color graphics printer to allow an engineer to configure, download, monitor, trend, document, modify, and verify system software configuration. The engineer's workstation should provide the ability to develop configurations in an on-line or off-line mode, with or without being linked to the DCS system. The engineer's workstation should display color graphics and all other information available to the DCS.

2.5.3.2.3 Full travel (not membrane), "QWERTY"-type keyboards may be provided on the engineer's workstation for configuration functions.

2.5.3.2.4 If an engineer's workstation is not available, then at least one operator station must offer the ability to configure all system functions.

2.5.3.3 Displays

The operator consoles should provide both *preformatted* displays and custom graphic displays. The preformatted display should be designed to allow easy setup.

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 the following paragraphs should be provided.

2.5.3.3.1 *Overview displays (preformatted):* Typically, overview displays should indicate both analog and discrete (on/off) values and contain at least 128 points per display. Operator control actions are typically not required from this display. Indication should be provided showing a displayed-point alarm status.

2.5.3.3.2 *Engineering displays (preformatted):* Engineering displays should 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.

Off-line configuration is typically preferred, in which case engineering functions may be done using a personal computer.

COPYRIGHT 2002; American Petroleum Institute

Document provided by IHS Licensee=Sincor Venezuela/5934214100, User=, 08/13/2002 12:13:45 MDT Questions or comments about this message: please call the Document Policy Management Group at 1-800-451-1584.

2.5.3.3.3 *Group displays (preformatted):* Group displays should indicate both analog and discrete (on/off) values and typically contain at least eight points per display. Indication must be provided, typically a faceplate, showing any displayed-point alarm status. Operator actions should be possible from this display. Common operator actions include the following:

a. Control functions:
   1. Mode—auto/manual/cascade/computer selection.
   2. Setpoint change.
   3. Output change (in manual).
b. Discrete functions:
   1. Auto/manual and computer selection.
   2. Force on or off (in manual).
   3. Reset (counters, timers, and the like).

2.5.3.3.4 *Detail loop displays (preformatted):* 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.

2.5.3.3.5 *Trending displays (preformatted):* Trends display any selected data stored in the history system. This data may be real time or historical. It should be possible to trend at least four variables on a single display.

Operator ability to change on-line, scaling, color selections, and the time period viewed is recommended.

At least ten such screens should be operator configurable to the extent that the operator may select the points to be stored and trended.

It is often beneficial to combine trend displays with group or graphic displays.

2.5.3.3.6 *Custom graphic displays:* Any point, measured or calculated, should be capable of being displayed on a custom graphics display as an active variable. A minimum of 128 dynamic points should be able to be displayed on each graphic screen. No high-level language programming, nor a host computer, should be required to create or display graphic screens.

The configuration of graphic displays should be interactive. Capacity for a minimum of 200-user graphic displays should be provided. It is recommended that ANSI/ISA S5.5 graphic symbols for process displays be used for the development of graphic displays.

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.

The operator should be able to manipulate any control loop, device, batch procedure, and so forth, from a graphic display.

2.5.3.3.7 *Sequence detail display (batch operation):* The sequence detail display should provide information required for monitoring and manipulation of an individual sequence. This display allows changes to the sequence such as step manipulation or alterations to the sequence state or status. The sequence detail display contains information such as sequence ID, batch ID, recipe ID, unit ID, current step, step time, step paused, and so on. Loop information related to the sequence and unit are also displayed.

2.5.3.3.8 *Utility displays:* Utility displays should show all system functions, such as formatting disks.

2.5.3.3.9 *Diagnostic displays:* 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.

2.5.3.3.10 *System status displays:* A system status display on the operator's console should summarize the status of each of the components connected to the system. Failures in it 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.

2.5.3.3.11 *System configuration displays:* System configuration displays should provide information about the configuration of system hardware and software. Displays can include the following as a minimum:

a. A display which shows the titles of all display groups available.
b. A display which shows all tag names, numbers and groups to which they are assigned.

2.5.3.4 Reports and Logs

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

A text editor is required to develop reports. The editor must be capable of doing custom formats using any of the system database variables.

2.5.3.4.2 *Event logging:* An event logger should store messages for future reports and displays. Each event should have the current date and time stored with it. The events to be logged include these: device restart/reboot, system errors/alarms, use of a keylocked function, and alarm messages.

An event log display should be provided to display all events logged.

2.5.3.4.3 *Operator action logs:* The operator action log should include set point, mode (auto/manual/cascade), output changes for PID control functions, force on or off for

COPYRIGHT 2002; American Petroleum Institute

Document provided by IHS Licensee=Sincor Venezuela/5934214100, User=, 08/13/2002 12:13:45 MDT Questions or comments about this message: please call the Document Policy Management Group at 1-800-451-1584.

discrete functions, and other similar types of actions. This log should also log changes to tuning constants. It is preferred that this log be kept on a hard disk and provide a printed report on demand.

2.5.3.5 Alarm Management

2.5.3.5.1 *Alarm display capabilities:* Alarm functions should be provided. These functions should include (a) out-of-service, (b) out-of-range (high, low, open-circuit, and certain user-configuration contact statuses), (c) absolute high and low with deadband, (d) rate-of-change with deadband, (e) output high and low with deadband, and (f) contact input and output status alarms. The adjustment of any alarm value/deadband/time/disabling should be protected by security access level.

2.5.3.5.2 *Alarm annunciation:* The control system should continuously monitor all process variables for alarm conditions. Alarms refer to any system diagnostic alarms or process alarms including the failure or disconnection of any device in the control system.

The colors used for alarming should be exclusive on displays for consistency and visibility within a system.

There should be common alarm acknowledge capability within a console. Critical alarms may be individually acknowledged or cleared in order to silence the audible signal.

2.5.3.5.3 *Critical alarm displays:* A dedicated critical alarm display should be provided. The critical alarm display should indicate the status (active or clear) of each and every critical alarm and must be updated in real-time. This may be a hardwired annunciator.

2.5.3.5.4 *Alarm identification:* Loops in alarm should be identified on displays by a user-specified color change. Unacknowledged alarms shall be indicated on displays by a flashing color change. The type of alarm (absolute, deviation, and so on) may be shown on the loop faceplates or group displays.

2.5.3.5.5 *Alarm priorities:* A minimum of four levels of process alarm priorities should be provided, such as critical, important, abnormal, and information/status. Each priority level shall have a unique visual and audible annunciation.

2.5.4 DATA HISTORIZATION

The DCS system should be provided with the capability to accumulate and store process information history.

This data should be selected from all points within the system, including analog values, measured or calculated, and discrete status points, measured or computed. Several sample rates should be available for selection. At least 30 days of storage space should be provided, on-line, for process data. Floppy disk or tape is not recommended for on-line storage. The system should provide for data archiving on removable magnetic or optical media. The system shall prompt the operator to insert a new removable media disk at least 12 hours prior to data being lost.

Sufficient capacity should be provided to acquire and retain *high-resolution* one-minute or faster data of all points simultaneously for 24 hours.

2.5.5 CONTROL FUNCTIONS

2.5.5.1 Input Characterization

Input characterization functions include the following:

a. Analog input conversion, linearization, square root extraction, and scaling.
b. Automatic validity test and alarm (out-of-range limits).
c. Totalize analog input and pulse count input.
d. T/C - ISA types: B, E, J, K, N, S, and T.
e. Contact status.
f. RTD.

2.5.5.2 PID Functions

PID functions should include the following:

a. PID basic controller.
b. PID ratio.
c. PID cascade.
d. PID bias.
e. PID differential gap.
f. PID adaptive gain.
g. PID non-linear.
h. Manual station.
i. PID self-tuning.
j. External output tracking.
k. Reset limiting.

2.5.5.3 Math Functions

Mathematical computation functions should include the following:

a. Add.
b. Subtract.
c. Multiply.
d. Divide.
e. Summation (bias).
f. Difference.
g. Square root.
h. Square.
i. Absolute value.
j. Logarithm.
k. Exponential.
l. Polynomial.

2.5.5.4 Limit Functions

Limit functions should include the following:

a. Low select.

COPYRIGHT 2002; American Petroleum Institute

Document provided by IHS Licensee=Sincor Venezuela/5934214100, User=, 08/13/2002 12:13:45 MDT Questions or comments about this message: please call the Document Policy Management Group at 1-800-451-1584.

b. High select.
c. Low limit.
d. High limit.

2.5.5.5 Dynamic Functions

Functions to mathematically model process dynamics should include the following:

a. Lead/lag.
b. Dead time.
c. Velocity limit.
d. Totalize.

2.5.5.6 Miscellaneous Functions

Individual controller functions should include the following:

a. Bumpless transfer.
b. Ramp to set point.
c. Ramp of output.
d. Ramp of calculated values.

2.5.5.7 Alarm Functions

DCS alarm capabilities should include the following:

a. All analog inputs.
b. All analog outputs.
c. All internal values (for example, setpoints, ratios, selected values, and so forth).
d. Changes in state for all digital signals, both field I/O and internally generated, and command disagree.
e. Abnormal state of device handlers.
f. Activation and deactivation of alarming per point.
g. Reporting of current alarm states.

2.5.5.8 Logic Control

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, graphic displays, or Boolean statements.

Logic control functions should include the following:

a. And.
b. Or.
c. Exclusive or.
d. On/Off delay.
e. Inverter.
f. Flip-flop.
g. Pulse.
h. Nand.
i. Nor.

2.5.5.9 Batch/Sequence Control

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

2.5.6 CONFIGURATION AND PROGRAMMING

2.5.6.1 Configurable control functions should be available as standard algorithms, as a minimum. No programming should be necessary to implement these functions.

2.5.6.2 Configuration in the DCS system should be accomplished using a fill-in-the-blanks, graphical block diagram or conversational technique.

2.5.6.3 It should be possible to configure additional database points and control schemes while the system is on-line.

2.5.6.4 The system should have the capability to document the configuration by transferring the data to a storage device in a standard database format for off-line evaluation, storage, and documentation. The ability to generate the initial configuration from such an off-line database (without reentering data into forms) is a very desirable feature.

2.5.6.5 Configuration and its backup onto removable memory should be possible from a single terminal. Loading configuration should be a simple procedure. The system must be flexible to meet changing process conditions. A system that requires substantial reprogramming to modify the configuration should not be considered for process control.

2.5.6.6 Configurable and programmable mathematic computational functions should be provided in order to perform real-time calculations of control variables for use in feedforward and other control schemes. Facilities for calculating tuning parameters and process modeling constants should be provided.

2.5.6.7 Protected high-level programming language facilities should be provided to allow the user to develop specific application programs, for example, reports, control, displays, and data analysis. The preferred programming languages are Basic, Fortran, C, and Pascal. Appropriate editing, testing, and debugging tools should be provided.

2.5.7 FOREIGN DEVICE INTERFACE

2.5.7.1 General purpose digital communication interfaces should be provided to allow high speed information exchange between the DCS and other devices. The general purpose digital communication interfaces should provide user adjustable means of setting the following parameters: serial or parallel transmission, half/full duplex, parity, character length, number of start/stop bits, synchronous/asynchronous, bits per second (1200 and greater), protocol encoding method, and data security methods used. Communications software should be included.

COPYRIGHT 2002; American Petroleum Institute

Document provided by IHS Licensee=Sincor Venezuela/5934214100, User=, 08/13/2002 12:13:45 MDT Questions or comments about this message: please call the Document Policy Management Group at 1-800-451-1584.

2.5.7.2 Two types of general purpose digital communication interfaces are recommended:

a. An interface to process input/output devices such as tank gauging transmitters, programmable controllers, flow computers, and the like. The interface should be highly secure. Furthermore, this interface should allow data, analog or discrete, to be displayed at the operator's console, and to be freely mixed with other process data in graphics displays.

The interface must have bi-directional communication to allow all control functionality and programming capability through the DCS. The performance of interface for control and alarming functionality should be consistent with DCS performance as listed in Table 1.

b. A high-speed bi-directional interface to a computer. The interface should be secure and should allow all process data to be transmitted to the computer and allow the computer to transmit any request. A configurable means of securely preventing the interface from directly affecting process control must be provided.

These interfaces (hardware and software) should be standard, available, protocols and have standard port configurations. Computer and DCS vendors must be consulted to provide the correct hardware and software.

2.5.8 COMMUNICATIONS

2.5.8.1 Communications Security

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

a. Error detection and correction on all data transfers.
b. Automatic retransmission in the event of errors and alarming on a failure after a suitable number of retries.
c. Continual checking of the back-up communication cable.
d. Automatic switchover to the back-up communication cable and alarm upon failure of the main communication cable.

2.5.8.2 Peer-to-Peer Communication

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

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

2.5.9 SYSTEM PERFORMANCE

Fast response times are not essential for all DCS application, and can actually be confusing to the human users. Fast response screens must not be substituted for an adequate number of screens which may be needed to provide a continuous overview of the process.

Recommended time periods to accomplish specific system functions are shown in Table 1.

2.6 Testing

A complete and comprehensive test program should be performed. Testing may be performed in four major categories as listed in the following, depending upon the size and complexity of the system.

a. Manufacturing testing.
b. System staging/integration.
c. Factory acceptance test.
d. Site acceptance test/operability evaluation.

2.6.1 MANUFACTURING TESTING

2.6.1.1 Standard tests on all components and subassemblies should be performed in accordance with accepted industry quality assurance practices.

Table 1—Time Period for System Functions

Event	Recommended	Maximum
Data acquisition display	1.0 sec.	3.0 sec
Alarm event reporting	<0.2 sec.	0.5 sec.
Time tagging of selected(alarm first out capability)	0.005 sec.	0 .010 sec.
Call-up a graphic display (250 dynamic variables)	<2.0 sec.	4.0 sec.
Display refresh	1.0 sec.	4.0 sec.
Time delay from command entry at workstation to field device start	<0.2 sec.	2.0 sec.
Plant overview information	1.0 sec.	2.0 sec.
PID loop controller	0.02 sec.	1.0 sec.
Call-up an eight faceplate display	1.0 sec.	2.0 sec.
Call-up a four variable trend display	<2.0 sec.	3.0 sec.
Analog output update	0.2 sec.	1.0 sec.

Note: All of the performance requirements should be met even under conditions of peak loading, such as large changes in many process variables at once, many points going into alarm at once, simultaneous requests for new displays from most display terminals, and printing reports.

COPYRIGHT 2002; American Petroleum Institute

Document provided by IHS Licensee=Sincor Venezuela/5934214100, User=, 08/13/2002 12:13:45 MDT Questions or comments about this message: please call the Document Policy Management Group at 1-800-451-1584.

2.6.1.2 Records of system tests should be available for review.

2.6.2 SYSTEM STAGING AND INTEGRATION

2.6.2.1 All finished components and subassemblies should be assembled in one area to test the system as an integrated system.

2.6.2.2 The completed system should undergo an operability test and remain 100 percent operational for a minimum of 100 consecutive hours with no software or hardware failures.

2.6.2.3 System hardware testing should cover the following areas:

a. Visual inspection of all components, including wiring, hardware location, access, and proper labeling, and physical assembly.
b. Continuity check of termination panels and interconnecting cables.
c. AC and DC power checks.
d. Proper operation and switching of backup devices.
e. Proper operation of the communication network under full load.
f. Diagnostic checks on all devices.

2.6.2.4 System software testing should cover the following areas:

a. Run standard diagnostic tests for system hardware and software functions, security performance, and software functions.
b. Load and verify all databases and displays for physical presence and proper linkages.
c. Check communications for proper operation and monitor for excessive errors.

2.6.2.5 All deficiencies and problems that arise during system staging should be corrected by the vendor prior to the factory acceptance test.

2.6.3 Factory Acceptance Test

2.6.3.1 The factory acceptance test is to verify that the system and its components function properly, that all manufacturing, assembly, software generation, and configuration have been done correctly and completely, and that system performance is in compliance with the agreed upon procurement specifications.

2.6.3.2 The factory acceptance test immediately follows the completion of system staging.

2.6.3.3 The factory acceptance test should cover the following areas:

a. Communication subsystem test: The overall security system is verified by forcing a failure of the communications path, cable, and power to verify the proper system operation under each condition. The communications subsystems are tested from each master to each slave and from master to master. The communications test will verify all possible communication paths, including primary and redundant networks and cables. Appropriate error conditions will be forced to ensure proper communication path switching upon failure.
b. Software loading and backup procedures: These procedures shall be demonstrated.
c. Security access: The view-only, operator, supervisor, and engineer keylock and/or password security access system should be checked for proper operation.
d. Foreign equipment interface testing: The vendor should propose methods for testing interfaces to the process computer, PLCs, and the like. The proper operation of the interfaces should be tested and verified prior to the end of the factory acceptance test.

2.6.3.4 The following can be tested if a system database has been generated:

a. Displays and reports: All displays and reports should be requested and checked for format, content, and operation. This test includes the standard displays and all graphics. All reports should be tested for format and content both on the CRT screen and on printouts. All historization, trending, alarming, and printing should be tested.
b. Tag function testing: The following testing should be performed for all tag points in the system.

1. Analog inputs and outputs: 0, 25, 50, 75, 100 percent of scale accuracy test (a random sampling of inputs and outputs can be tested for accuracy if the system is large or time is limited).
2. Discrete inputs and outputs: change of state.
3. Proper algorithm.
4. Control action.
5. Alarm limits.
6. Alarm action.
7. Manual/auto/cascade mode switching.
8. Graphic representation.
9. Scaling coefficients.
10. Trends.

c. Item b must be done in total at least once during the project. Tag points may be tested by simulating an input at the I/O, observing the readout at all displays associated with the point, and verifying an output (when applicable) at the point. Tag function test results should be verified.

2.6.4 SITE ACCEPTANCE TEST AND OPERABILITY EVALUATION

2.6.4.1 A test of the system should be conducted as soon as it has been installed at the job site in its final configuration. This test should repeat the factory acceptance test or an acceptable subset of the test to verify that no damage occurred during shipment and installation. Some items may be covered during loop calibration and checkout.

COPYRIGHT 2002; American Petroleum Institute

Document provided by IHS Licensee=Sincor Venezuela/5934214100, User=, 08/13/2002 12:13:45 MDT Questions or comments about this message: please call the Document Policy Management Group at 1-800-451-1584.

2.6.4.2 The system must demonstrate the performance of necessary system functions and meet the specified availability requirements. The evaluation should be performed after the completion of the site acceptance test. This evaluation demonstrates that the system has been completed. The operability evaluation is considered successful with performance of 99.9 percent availability within a continuous 1000-hour period.

2.7 Documentation

2.7.1 The vendor should include a list of the publications that are available and needed for the operations and maintenance of the system. Documentation should be available in hardcopy form. The availability or use of electronic documentation should not release a vendor from the requirement providing documentation in hardcopy form. The documentation included on the list should meet the following minimum requirements:

2.7.2 Documentation should be coherent and consistent from one document to the next. Documents shall be fully indexed and cross-referenced.

2.7.3 The issue number and date of issue should be stated on every page of each document. Changes from previous issues should be clearly identified.

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

a. Equipment startup/shutdown procedures.
b. Routine maintenance procedures.
c. Routine preventive maintenance procedures.
d. On-line and off-line diagnostic and testing procedures.
e. Normal and trouble condition of all diagnostic indicators.
f. Location of all voltage test points and nominal values.
g. Reference to interpret the meaning of all status codes and alarms.
h. Site planning, hardware installation, and grounding.

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

2.7.6 A hardware manual should include the following:

a. Complete bill of material for all items.
b. Statements of system and subsystem functions, of design strategies, and of constraints.
c. Description of the hardware configuration.
d. Description of operation, including operation of each component board.
e. Equipment specifications.
f. Inter/intra cabinet cabling drawing(s): All cables are to be referenced by name and/or part number. All drawings shall reference cable and conduit schedules.
g. Cabling between consoles and cabinets: These drawings shall include pin-out definitions, wiring colors, and cable name/model numbers and all jumpers between mounting structures and/or cable termination points.
h. Foreign equipment interface cabling: These drawings should include all wiring and connections between the interface devices.
i. I/O termination wiring and cabling drawings: These drawings shall include a wiring schedule/drawing identifying each terminal in the DCS enclosure(s) and its connection path to all connections prior to entering an I/O processor. Information on the I/O module name or number, channel, and wire definition (namely, +, –, + power, or shield) shall be included.
j. Details of cabinet layouts including dimensions and weights.
k. Power supply and grounding requirements.
l. Heat dissipation ratings and environmental limitations for all equipment.
m. Details of all interfaces to other vendor's equipment.
n. Spare parts information.

2.7.7 Where a foreign device interface is programmable or configurable, a manual must provide clear, complete written documentation on the following:

a. Design philosophy.
b. Technical description of the software/configuration.
c. Language in which the program is written.
d. System flowcharts and dataflow diagrams.
e. A well-annotated program/configuration listing.
f. A description for program linkage, including activation modes, parameters passed, and termination mechanisms.
g. A definition of data structures (internal and external) used.
h. System utilities for documenting the contents of the system and managing its development.
i. Software/configuration loading, backup, and downloading procedures.
j. Software/configuration diagnostic aids, performance monitoring utilities.
k. A list of all alarms and messages produced by the software or configuration.
l. Initialization/restart requirements.

COPYRIGHT 2002; American Petroleum Institute

Document provided by IHS Licensee=Sincor Venezuela/5934214100, User=, 08/13/2002 12:13:45 MDT Questions or comments about this message: please call the Document Policy Management Group at 1-800-451-1584.

SECTION 3—ALARMS AND PROTECTIVE DEVICES

3.1 Scope

This section recommends systems, installation considerations, and testing procedures for alarms and protective devices used in refineries.

3.2 Referenced Publications

The latest edition or revision of the following publications shall, to the extent specified, form a part of this recommended practice (see 1.4 for publication data): API RP 750, RP 556, API 551, Std 612, Std 614, Std 616, Std 617, Std 618, Std 619, Std 674, Std 675, and STD 676; ISA RP 12.4 and SP 18.1.

3.3 General

A large number of process variables and equipment parameters are monitored for abnormal status in petroleum refineries. Alarms announce off-normal conditions to alert operations personnel of impending or actual processing unit problems. Protective devices take action to eliminate a potentially hazardous condition before it can cause injuries to personnel, damage equipment, or harm the environment.

This section focuses on the functionality of alarms and protective systems rather than the design aspects of the system itself. Consideration should be given to the role of hazard analysis, risk assessment, failure mode considerations, design concepts, test frequency, and the like. Reference should be made to API RP 750.

There are several types of alarm and alarm systems associated with typical refinery control centers. These are as follows:

a. *Process alarms*, such as flows, levels, temperatures, analyzers, and calculated process parameters to alert operators to off-normal process parameters or production targets.
b. *Equipment monitor alarms*, such as bearing temperatures, to alert process operators of mechanical problems on process equipment.
c. *Diagnostic alarms* monitor performance characteristics of the control, communications, and operator interface of distributed digital control systems or other process computer-based control systems.
d. *Ambient monitor alarms,* such as area monitors for fire, toxic/flammable vapors, and environmental hazards to reduce risks to personnel.
e. *Sequence of events (SOE)* provides high-speed scanning of a group of alarm points associated with a process unit. SOE alarms help determine the sequence and initial cause of failure on process equipment such as boilers, compressors, turbines, or other equipment.
f. *Events monitoring*, discrete events such as operator initiated control actions, system mode changes, and application program events as generated by higher-level supervisory programs.
g. *Override control/safety shutdown* to protect process equipment, prevent harmful environmental discharges, and provide personnel safety. These are included in control strategy configurations to automatically initiate override controls or safety shutdown systems.

Process alarm points are to be judiciously selected to provide meaningful information to the operators and control system strategy. The temptation to include superfluous alarms in systems design should be resisted. Operators will consider these as nuisance alarms which may result in inattention to more critical alarm conditions.

Distributed control systems (DCS) allow for multiple levels of alarm prioritization. Alarms of higher priority should be acknowledged and acted upon before lower-priority alarms.

DCS can also provide an alarm history package allowing operations management to obtain alarm history reports for specific process areas and past time intervals to assist in analyzing unit process performance.

3.4 Alarm Systems

Alarm annunciators and display systems can be classified into two broad categories:

a. *Dedicated* alarm annunciator and display systems wherein each alarm point is self-contained and grouped with other points in dedicated hardware, typically with back-lit engraved windows or alarm lights to indicate the point or area of alarm.
b. *Integrated* alarm and annunciator systems are commonly included in CRT-based control systems. Alarm processors, displays, and alarm logging printers are common in DCS.

3.4.1 DEDICATED ALARM SYSTEMS

A dedicated alarm system usually has a separate visual indication for each alarm point as well as a separate actuating device (see Figure 2). In some cases, it may be practical to combine a number of actuating devices so that operation of any one of them would produce an indication on a common remote visual alarm. The alarm point of the sensor is determined either by a setpoint adjustment (such as in a pressure or temperature switch) or by installation location (such as for a level switch).

Electrically operated devices are commonly used for dedicated alarms. Nevertheless, some pneumatic systems are employed in areas where power may not be available or where electrical equipment could constitute a hazard. Electrical alarm contacts are then actuated by pneumatic pressure switches, either located in a safe area or manufactured to meet the area classification.

COPYRIGHT 2002; American Petroleum Institute

Document provided by IHS Licensee=Sincor Venezuela/5934214100, User=, 08/13/2002 12:13:45 MDT Questions or comments about this message: please call the Document Policy Management Group at 1-800-451-1584.

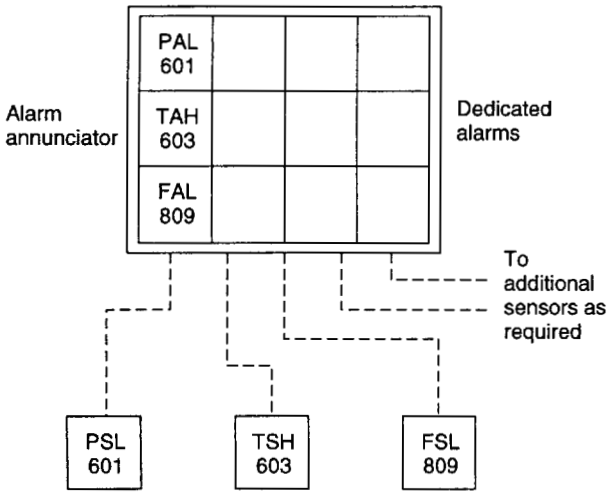


Figure 2—Schematic Showing Dedicated Alarm System

The alarm point is identified by illuminating a translucent, back-lighted nameplate describing the alarm. The nameplates (or windows) are available in multiunit cabinets that are usually self-contained, that is, the cabinet contains the necessary power source and requires connections only to the alarm switches. In some instances, single-alarm lights located in a panel or an instrument may provide sufficient visual indication.

Another configuration is to mount the alarm electronics remote from the alarm light display.

Color coding of the windows or alarm lights can be used to identify (a) the seriousness of the alarm condition or (b) the section of the plant in which the alarm has occurred.

An audio signal is provided when any one of the alarm points is actuated. This audio signal will alert the operator to look at the visual indication for identification and evaluation.

Dedicated alarms can also accept analog inputs in the form of current, voltage, or direct thermocouple and resistance temperature detector signals. The alarm trip point and dead band are determined by integral adjustments for each input. Dedicated alarm systems may be capable of outputs via auxiliary contacts or data communication links. Dedicated alarms are usually located in the control room and may be mounted on the instrument panel on the operator's console, or the annunciator may be suspended from the ceiling.

In some instances, it is advisable to locate an annunciator cabinet with audible alarms in an area close to the equipment that is being monitored. This configuration could be used for compressors and furnaces to ensure prompt action on the part of field operators. A common-trouble alarm should be provided in the control room. Depending on area classification, it may be necessary to provide an explosion-proof annunciator or purged annunciator enclosure (see ISA 12.4). The selection of the alarm system must always comply with the electrical classification of the area in which the system is to be installed.

3.4.2 INTEGRATED ALARM SYSTEMS

Integrated alarm systems can be in the form of stand-alone scanning and alarm-only units or an integral part of larger distributed digital control systems (see Figure 3).

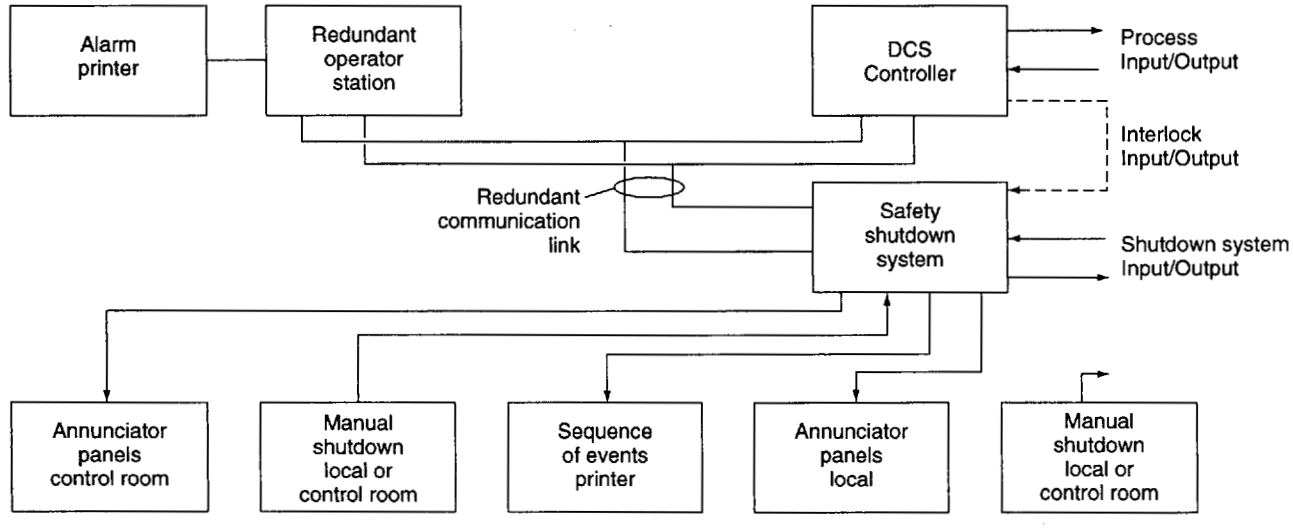


Figure 3—Schematic Showing Integrated Distributed Control System Alarm and Safety Shutdown System

COPYRIGHT 2002; American Petroleum Institute

Document provided by IHS Licensee=Sincor Venezuela/5934214100, User=, 08/13/2002 12:13:45 MDT Questions or comments about this message: please call the Document Policy Management Group at 1-800-451-1584.

System inputs may be hardwired analog signals with the distributed system checking for the high, low, deviation, or rate of change alarm conditions configured for each point, or field-mounted alarm switch contact closures wired directly to the distributed system's discrete input modules, or a separate programmable logic controller (PLC) communicating with the DCS via a separate communication link.

Distributed systems facilitate the development of computed alarms such as may be generated by a sequence of discrete events or computed values.

Distributed control systems offer a variety of alarm handling features and capabilities for conditioning and presenting alarms in an efficient way. These methods protect the operator from being overwhelmed by an inundation of alarms during process upsets. The logical processing of events also aids the operator in quickly assessing inputs and emergencies so that appropriate corrective action can be taken.

Alarm conditioning methods should include consideration for the following:

a. Priorities: Alarms are configured on a numerical priority for each point based on relative importance, for example, safety alarms are high; maintenance alarms are low. At least three levels of priority should be provided. Priorities can be designated on the process and instrument diagram (P&ID) for each alarm.
b. Groups: Alarms are segregated into user groups of associated function, for example, safety, process areas, security, diagnostics, and the like.
c. Modes: Alarms may be assigned different attributes depending on the selected operating state, for example, start-up, normal, no alarm, shutdown, and so forth.
d. Variable attributes: The action taken when an alarm occurs can vary, depending on the operating mode and assigned group. Some of these attributes are sound horn, print occurrences, screen display, and generate message.
e. Blocking: This is the capability to selectively suppress alarms which are faulty. A *defeated alarms* list must be provided in the system. Some security measures should be provided with this capability.
f. Conditional acknowledge: This is the ability to acknowledge all alarms from a group or the entire system after a major event occurs, such as plant-wide power failure. This circumvents the normal procedure of individually selecting and acknowledging each alarm.
g. Conditional suppression: Relational logic may be applied to associated alarms to eliminate multiple reporting of a single event; for example, if a motor shuts down, a downstream low-pressure alarm may be suppressed.
h. Fixed or adjustable deadband: Alarms should be configured so that if a process variable is operating around a setpoint, the process variable will not continuously oscillate in and out of alarm.
i. Computed alarms control display pointers (optional): An alarm may be generated based on a logical combination of states, conditions, and events. An alarm point may be linked to its associated interactive process control display. This allows automatic display callup by merely acknowledging the alarm.
j. Help files (optional): Preformatted messages may be associated with alarms to aid the operator in understanding the occurrences and/or to make recommendations on responsive action.
k. Expert systems/artificial intelligence (optional): The system may analyze alarms and inform the operator, through messages, of the probable cause(s), make recommendations on a course of action, and provide operational alternatives.

The DCS operator receives information from and interacts with the system through various devices on the console. In addition to the CRT displays, the following information sources should be considered:

a. Audible indication: Tones may vary according to the relative importance of the alarm, or the physical location; a minimum of two are recommended.
b. Chronological printouts: These are to aid the operator in analyzing the alarm sequence and to provide a hard copy record of the alarms.
c. Dedicated access method: Special function keys or touch screens can be configured on the console so that when an alarm which was assigned to that key occurs, the key is lit to alert the operator. Upon pressing that key, a preassigned display may appear or some automatic process action or sequence may be initiated.
d. Alarm history: Alarm events are placed in memory which allows retrieval, formatting, and the reporting of events by the process unit for historical analysis. In addition to process control alarms, historical events may include operator-initiated actions, such as control actions (for example, setpoint changes) or mode changes (for example, auto/manual switching), systems alarms, application-program-generated events, and sequence-of-events process equipment monitoring.

3.4.3 METHOD OF OPERATION

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

The operating sequence described in Table 2 is the most common, although many different ones are available (refer to ISA 18.1).

COPYRIGHT 2002; American Petroleum Institute

Document provided by IHS Licensee=Sincor Venezuela/5934214100, User=, 08/13/2002 12:13:45 MDT Questions or comments about this message: please call the Document Policy Management Group at 1-800-451-1584.

Table 2—Typical Alarm Operating Sequence

Signal Device	Normal	Alarm	Acknowledge	Return to Normal
Visual	Off	Flashing	Steady on	Off
Audible	Off	On	Off	Off

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

In CRT-based systems, an alarm message is usually displayed on the screen in a prominent location, possibly flashing or appearing in a distinguishing color. An audible device may also sound. One or more acknowledge buttons are provided to acknowledge the alarm condition. In some systems, the button will also call up a related display with additional information relative to the alarm condition. A logging system may be actuated to document the alarm message.

3.4.4 AUDIBLE INDICATION

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

Audible signals are in the form of bells, buzzers, horns, or electronic devices. These audible signals may be differentiated so that either the location in the refinery or the seriousness of the condition can be indicated. For example, some may merely indicate an upset condition, while others indicate to the operator that a shutdown has occurred. Shutdown alarms commonly are designated to initiate an audible signal distinct from all other alarms.

3.4.5 TESTING

Alarm systems should be installed to facilitate testing of individual alarms during the operation of the process unit. Individual alarm points should be tested by activating the primary sensors. Test schedules, procedures, and results should be documented. The frequency of testing should be determined by the criticality of the alarm and the service history of the device.

3.4.6 SAFETY CONSIDERATIONS

Selection of reliable equipment, proper installation with respect to recommended practices and codes, and regular maintenance are important safety considerations and should be applied to alarm installations. In some instances where a high degree of reliability is required, it may be required to install multiple alarm devices.

3.4.7 DOCUMENTATION

A complete and accurate record of all alarm setpoints should be maintained. It is useful to combine this with the test procedures (3.4.5). This record is necessary when checking out initial installations, for testing, and for communicating changes that might be made in the course of system operation. Recommended database information should include tag number, service description, alarm setpoint, dead band, and P&ID or loop-drawing numbers.

3.5 Protective Systems

The function of protective instrumentation is to recognize a potentially hazardous situation and take corrective action before it can cause injuries to personnel, damage to equipment or the environment, and the loss of production.

The primary devices used to detect the hazardous conditions are, in most cases, similar to those used to generate alarms. However, the protective system, in addition to operating a visual and/or audible alarm, also transmits a control signal to a valve, motor starter, or other control device that will reduce the hazard by corrective action or process shutdown. High-quality components should be used throughout the protective system to ensure the highest reliability. Attention must be paid to material selection, failure mode, adequate testing features, design, and installation to ensure the reliable operation of the system.

The quality of the power supply for each protective system must be such that it will not adversely affect the reliability of the system. Power supply circuits for protective systems should be separate from power supply circuits for alarms and other control systems. Uninterruptible power supplies (UPS) should be considered.

The logic function for protective systems can be accomplished using hardwired, discrete components such as relays, timers, and switches. Solid-state logic systems, programmable controllers, or other microprocessor-based systems are also used in protective systems throughout the refining industry. The shutdown and control functions should be in separate and independent hardware which may share common operator displays with the DCS.

Redundant and/or fault tolerant designs should be considered, especially for microprocessor-based systems in critical service, as these systems cannot be designed to always fail in a safe direction. Protective systems should meet target availability and reliability criteria based on process hazards analysis. Non-redundant systems are acceptable when risks are less.

The shutdown by one protective system often affects other units in the process and may lead to activation of other protective systems. Such interaction should be analyzed and the systems coordinated to ensure a safe and controlled shutdown.

COPYRIGHT 2002; American Petroleum Institute

Document provided by IHS Licensee=Sincor Venezuela/5934214100, User=, 08/13/2002 12:13:45 MDT Questions or comments about this message: please call the Document Policy Management Group at 1-800-451-1584.

API RP*554 95 ■ 0732290 0549586 677 ■

3.5.1 TYPES OF PROTECTIVE SYSTEMS

The following examples (also see Figures 4 and 5) are not intended to be all inclusive. There can be many other applications of protective systems that ensure against hazards to personnel, damage to equipment or the environment, and loss of product.

a. *Compressors*: Typically, compressors are shutdown by either tripping the motor drive or closing the steam valve to the turbine drive. A protective system to accomplish the shutdown can be initiated if selected variables, such as level in a suction knockout drum, vibration, lubrication flow, seal fluid pressure, and so forth, exceed limits. See API Stds 612, 614, 616, 617, 618, and 619 for additional details.

b. *Fired heaters*: The function of the protective system for fired heaters is to shut off fuel to the furnace if selected variables exceed safe limits. See API RP 556 for specific recommendations.

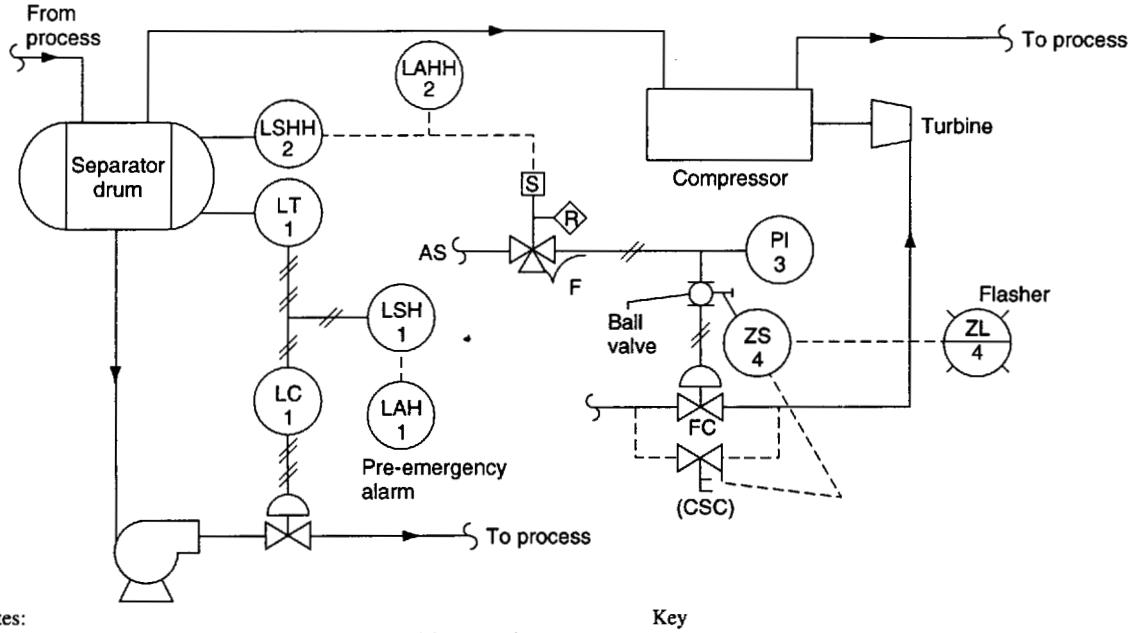
c. *Pumps*: In some cases, a protective system is installed to start up a standby pump if the primary pump fails. Detection of the failure can be through a measurement of low-discharge pressure or low flow through the pump. With large pumps, low flow may cause damage from heating or vibration, in which case the low-flow device may open a bypass valve or initiate a pump shutdown.

When pumping out of tanks, a protective system can be installed to initiate pump shutdown on low level to protect the pump from damage due to cavitation (see API Stds 674, 675, and 676).

d. *Reactors*: There are different types of catalytic reactors in petroleum refineries. High-catalyst-bed temperature, low-coolant flow, and low-feed flow are examples of conditions that would be monitored by protective systems. In the event that any one variable limit is exceeded, a number of functions can occur, such as shutting off fuel to the heat source, introducing a quench, diverting or interrupting feed, and so forth.

3.5.2 SENSOR CONSIDERATIONS

Protective system sensors must be highly reliable. Sensors may be switches or transmitters. Critical protective systems should consider redundant sensors to meet system reliability requirements. Consideration should be given to trouble shooting, calibration, and ease of replacement of sensors. To achieve reliability, an independent, direct-connected sensor is



Notes:
1. LAH1—pre-emergency high-level alarm actuated from monitor switch LSH1.
2. LAHH2—shutdown high-level alarm actuated by direct-connected level switch LSHH2. LSHH2 simultaneously de-energizes solenoid valve S, shutting off steam to the turbine.
3. Closing ball valve in steam valve air line or opening the bypass valve permits testing of shutdown system without interrupting process. Position switch (ZS4) actuates flashing light (ZL4) in control room to alert operator that system is in test mode. Pressure gauge (PI3) in air line indicates proper solenoid operation.

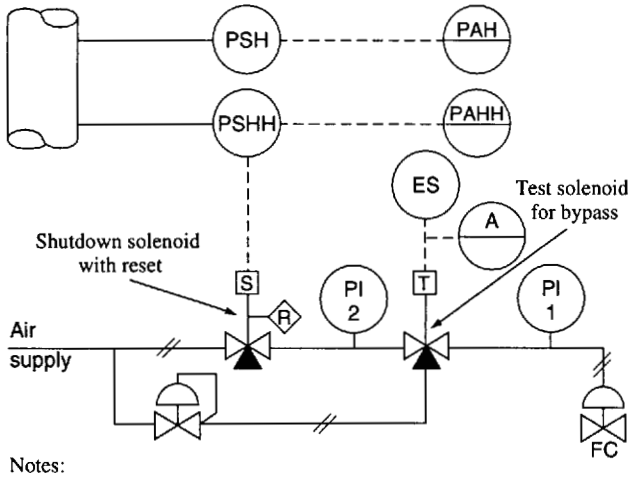
Key

AS	air supply	LT	level transmitter
CSC	car-sealed close valve	PI	pressure indicator
FC	fails closed	R	solenoid reset
LAH	high-level alarm	S	solenoid
LAHH	high-high-level alarm	ZL	flashing light
LC	level controller	ZS	position switch
LSH	high-level sensor	F	failure direction
LSHH	high-high-level sensor		

Figure 4—Typical Protective System With On-line Testing Capabilities

COPYRIGHT 2002; American Petroleum Institute

Document provided by IHS Licensee=Sincor Venezuela/5934214100, User=, 08/13/2002 12:13:45 MDT Questions or comments about this message: please call the Document Policy Management Group at 1-800-451-1584.



Notes:
1. Power alarms separately from shutdowns.
2. System shown in normal operation.
3. Bypass shutdown solenoid valve by energizing test solenoid routing a reduced air supply to the shutdown valve to test the shutdown system through the shutdown solenoid. Pressure gauges PI1 and PI2 indicate proper operation of the solenoid valves.
4. Annunciate shutdown bypass in control room.

Key

A	alarm for shutdown bypass
PI	pressure indicator
FC	fail close
PSH/PAH	pressure switch high/pressure alarm high
PSHH/PAHH	pressure switch high high/pressure alarm high high

Figure 5—Typical Protective System With Testing Feature

employed to monitor the measured variable and initiate the automatic action. Such a device is not dependent on any other piece of equipment or system for its function. This sensor should be connected independently to the process and not share impulse piping or valving with any other device. The sensors are typically applied in a de-energize-to-trip configuration such that automatic action is initiated upon sensor, signal, or power failure. If energize-to-trip systems are installed, more frequent scheduled testing may be required.

3.5.3 SHUTDOWN ALARMS

All shutdown initiating functions should also be annunciated to determine the cause of the event. The activated safety device and alarm annunciating circuit must be electrically isolated. In many cases, a different audible signal is used to distinguish the protective system alarm from an ordinary alarm. First-out alarm displays or sequence of events (SOE) recorder reports with time tagging are suggested to identify the shutdown events.

3.5.4 PRESHUTDOWN ALARMS

The activation of a protective system usually causes a shutdown of process equipment. It is recommended practice to provide a preshutdown process alarm to enable the operator to take corrective action before the protective system is activated. This alarm should be a separate annunciated point, typically on the DCS.

3.5.5 FINAL CONTROL ELEMENTS

Field devices used in conjunction with protective systems are usually electrically activated. Some pneumatic and hydraulic devices are used where electrical power is either restricted or unavailable or where a specific requirement exists to render the system independent of electrical power.

The most commonly used items are solenoid valves, applied directly to the process for control of fluid flow, or used to vent or admit instrument air to air-operated control elements.

Final control devices for protective systems should typically be of design such that the intended protection action occurs upon component, signal, power, or pneumatic failure.

Protective devices can start and stop pumps, compressors, or conveyors to ensure a return to safe process conditions.

In most cases where a protective system is installed, a manual reset feature must be provided. This system should take the form of a mechanical or electrical *latching* arrangement that requires manual intervention to reset the system. If this reset feature is not provided, potentially dangerous cycling might occur. When mechanical latches are provided, provisions must be made in the administrative procedures to prevent the defeating of the devices.

Input and output modules of protective systems in critical applications should be capable of detecting and alarming open- or shorted-field circuits.

3.5.6 LOGIC

The following considerations should be included in the design:

a. The memory of the system shall be non-volatile: That is, a power failure will not result in a loss of memory.
b. A method of system failure notification should be included in the design.
c. The design of the system should permit *hand* (manual) control to allow safe shutdown in the event of system failure.
d. The design shall be such that system devices should be standard *off-the-shelf* items, and should bear recognized certification authority approval (such as FM or UL) for the use intended, and verification of this should be provided.
e. Access to the controller/microprocessor programming shall be supervised to limit user ability to modify the program or force outputs. Procedures and/or systems should be provided to prevent unauthorized changes to the PLC logic.
f. The design of the system programming sequence and program operation shall be logical and clearly written. Documentation should be provided to verify the system software.

COPYRIGHT 2002; American Petroleum Institute

Document provided by IHS Licensee=Sincor Venezuela/5934214100, User=, 08/13/2002 12:13:45 MDT Questions or comments about this message: please call the Document Policy Management Group at 1-800-451-1584.

g. Emergency shutdown logic and process control logic should not be in the same system for critical applications.

3.5.7 TESTING

Protective systems may remain inactive for long periods during which contacts may corrode, wires may be broken, or mechanical linkages may cease to function. A means of periodically checking the entire protective system while the process unit is operating is desirable. Such systems should be inspected and tested as completely as practical on a scheduled basis. In addition the total system should be inspected and tested during plant shutdown periods. Trip systems that are difficult or impossible to test during operation should be tripped as part of a planned shutdown, assuring operability of those trip systems.

The sensor/initiating and display portion of the system can usually be checked with the unit operating; however, provision must be made to ensure that a shutdown does not occur when the sensor is activated. In the case of shutoff valves, either a valve in the air line or a piping bypass with a car-sealed, closed valve can be employed (see Figure 4). If possible, the test should include the final shutoff valve. The use of the car seals or chains ensures that the bypass valve is not inadvertently left open, nullifying the whole system. As a further precaution, a limit switch can be mounted on the bypass valve to operate a signal light as soon as the valve is cracked open. This light can be located in the instrument panel and could be colored or flashing to alert the operator that the protective system is being bypassed. Keylock switches or switch locations that discourage tampering should be used in this application. A panel-mounted indicating light can be used.

Bypass systems should be provided to facilitate testing the inputs and outputs of the system. When any bypass is in effect it should be annunciated in the control room or car seals and/or chains with locks used for proper management control. The shutdown system should remain operative except for the items bypassed. It is recommended that only one input or output is bypassed and tested at a time. In all cases the bypass system should be designed to keep the alarm circuits functional (as much as possible) during the testing period. Typical protective systems with testing features are shown in Figures 4 and 5.

Continuous self-checking features should be included in solid-state logic systems, programmable controllers, or other microprocessor-based systems. This feature reduces the probability of undetected failures that may cause dangerous system failures and create a plant hazard. Self-checking systems are usually of a proprietary nature and employ unique signaling and wiring techniques to detect and alarm failures in the system.

On-line diagnostics of the safety system should be provided to eliminate the need for special maintenance during plant shutdowns. Diagnostics should pinpoint the failed module. On-line replacement of failed modules should be possible.

Sensors should be tested in accordance with 3.4.5. Testing of protective systems is a means of ensuring a higher degree of reliability. Because of the need to provide bypass or deactivating features, testing caution must be exercised so as not to leave the system unattended while it is bypassed.

3.5.8 ENHANCING RELIABILITY OF PROTECTIVE SYSTEMS

Frequent testing and the use of multiple measuring devices, voting logic, redundant shutdown logic, and redundant final control elements achieve a significant improvement in the reliability. The investment cost will be greater, but the elimination, reduction, or simplification of testing procedures may warrant the added cost, as well as improving reliability and availability of the system.

3.5.9 DOCUMENTATION

For each protective system, a complete and accurate record of all shutdown trip setpoints should be maintained, along with proper documentation of corrective actions or shutdown functions performed at each trip point. This information will be needed when testing or troubleshooting a system and is necessary for communicating changes that might be made in the course of system operation.

There should be a formal system involving operations, safety, and engineering to approve and document setpoint and logic changes to shutdown systems (see API RP 750).

Protective systems should be fully documented, including configuration, logic documentation complete with annotations, operating, testing, and maintenance procedures.

3.6 Engineering Considerations

3.6.1 GENERAL REQUIREMENTS

The following practices are recommended for implementing process alarm and protective systems in refinery installations.

3.6.1.1 Process alarms should be shown on the P&IDs. Other alarms such as operator set deviation alarms, diagnostic alarms, calculated alarms, and the like, may be shown on other documentation.

3.6.1.2 Shutdown devices should be dedicated and separate from preshutdown alarm devices and the process control system.

3.6.1.3 Shutdown devices may actuate alarm devices provided the alarm circuits are electrically isolated from the shutdown circuit. This may be accomplished by clearly identified separate contacts in the process switch, an isolating relay, or the programmable logic controller.

COPYRIGHT 2002; American Petroleum Institute

Document provided by IHS Licensee=Sincor Venezuela/5934214100, User=, 08/13/2002 12:13:45 MDT Questions or comments about this message: please call the Document Policy Management Group at 1-800-451-1584.

API RP*554 95 ■ 0732290 0549589 386 ■

3.6.1.4 Critical shutdown alarms should be independent of DCS alarm systems such that a single failure does not affect both the DCS system and critical shutdown alarms simultaneously.

3.6.1.5 Manual initiation of the protective systems may be through switches wired directly to the shutdown final control element, to inputs wired directly to the protective system, or from the DCS operator console. The choice depends on the critical nature of the protective system and the distance separating the functions.

3.6.1.6 Procedures and/or systems should be provided to prevent unauthorized changes to protective system logic.

3.6.1.7 First out annunciation or event history recording should be considered to identify the cause of a shutdown.

3.6.1.8 De-energized-to-trip systems are preferred for high-risk systems such as personnel safety or environmental protection. Energized-to-trip systems may be considered for high-risk systems when nuisance trips due to system or power failure would cause a higher risk than a de-energize-to-trip system. For such systems, end-of-line device monitoring and frequent scheduled testing are recommended.

3.6.1.9 The following failure scenarios and the resultant effect on the systems shall be addressed and documented when microprocessor-based systems are used.

a. *CPU Stall*: The central processing unit (CPU) ceases to execute the program.
b. *Input-output (I/O)*: The I/O modules fail to scan input and output signals and instead base decisions on the last reported status existing in memory.
c. *Input failure*: Input module locks in the "on" or "off" position and does not respond to the action of the connected input device.
d. *Addressing device*: Failure of the program to correctly consult the input and/or external information sources.
e. *Output failure*: Output module freezes in the "on" or "off" position and will not respond to CPU instructions.
f. *Memory failure*: Failure of a memory register or a shift register which will cause an improper instruction to be given to the CPU.
g. *Watchdog timer failure*: Failure of the main oscillator controlling the execution of the program.

3.6.2 ELECTRICAL REQUIREMENTS

Good installation practice requires the use of a pair of wires to each field sensor. This simplifies maintenance and troubleshooting procedures and improves system security. Use of field common wires is not recommended.

Alarm circuitry should be designed to prevent interference with interconnected power and control circuits. This situation is especially of concern where common audible, acknowledge, or lamp-testing circuits are employed.

The quality of the power supply for each alarm system must not adversely affect the reliability of the alarm system. Alarm systems that are independent of DCS systems should be served from power supply circuits that are also independent from those that serve the DCS system.

Generally, alarm circuits from field sensor switches should be energized in normal operation. Normally energized system designs provide fail-safe characteristics. When energize-to-alarm systems are used, end-of-line devices capable of detecting open, short, or grounded connections should be considered.

Experience and good judgment must be combined in the selection of electrical contacts for relays and sensors. With the use of low-level direct current voltages in alarm circuits, hermetically sealed contacts are desirable to prevent the effects of dust, corrosion, and contact film. The corrosive effects of atmospheric contamination along with factors such as heat, vibration, and current rating must be evaluated in selecting electrical contacts. If mercury switches are used, they must be mounted where they are unaffected by vibration.

3.6.3 INSTALLATION

The installation of process-connected switches or transmitters should be made in accordance with the appropriate section of API RP 551 for flow, pressure, level, and temperature.

Dedicated-alarm annunciator systems installed in a control room should be positioned for maximum visibility and operator convenience. The relationship of alarms to other instrumentation may also be important. The proper location of the acknowledge pushbutton is important since it must be used by the operator after each alarm.

The audible device should be installed where it will attract attention but will not be unnecessarily loud.

Enclosures and wiring for the installation of alarm sensors must meet the requirements of the area in which they are located. Intrinsically safe systems eliminate the need for explosion proof enclosures for field sensors in classified areas. Hermetically sealed switch contacts eliminate the need for explosion proof enclosures that are otherwise required in Division 2 areas. Weatherproof enclosures are recommended for outdoor use with intrinsically safe systems and hermetically sealed switches regardless of area classification.

COPYRIGHT 2002; American Petroleum Institute

Document provided by IHS Licensee=Sincor Venezuela/5934214100, User=, 08/13/2002 12:13:45 MDT Questions or comments about this message: please call the Document Policy Management Group at 1-800-451-1584.

SECTION 4—PROCESS CONTROL COMPUTING ENVIRONMENT

4.1 Scope

This section covers the performance requirements, networks, hardware, software, and infrastructure associated with the process control computing environment. The intent of this section is to provide guidance to those parties developing detailed specifications for computing resources used for process control and associated functions in the petroleum industry. Plant computer and network architecture is introduced in this document to help define a process control computing environment. This document is based on the philosophy of using widely accepted computing industry standards and avoiding custom or proprietary approaches.

4.2 Referenced Publications

Note the following publications (see 1.4 for complete references): ARI Std 210, ASHRAE 15, *Standard Safety Code for Mechanical Refrigeration,* FIPS PUB 94 *Guideline on Electrical Power for ADP Installations;* IEEE 446; NFPA 70, 75, and NEC Article 440, UL 779, and API 750.

4.3 Plant Computer and Network Architecture

The plant computer and network architecture is shown in Figure 1. The architecture depicts several levels of computers and networks, with each lower level in the hierarchy responsible for narrower and more specific computing needs. The architecture is not intended to endorse or limit any specific computer and network architecture, and many variations are possible.

The architecture may also be expanded or contracted to fit the situation. For example, a large site might need to split the plant level into two levels; one which is sitewide and one which is for departments or divisions within the site. Conversely an enterprise with a single small site might condense the model's corporate and plant levels into one single level.

For ease of description, the term *process control computer* (PCC) is used throughout this document to refer to the entire process control computing environment. PCC functions operate at the unit level and/or the plant level due to the required high reliability and high availability. (see 1.5.2.)

As shown in the architecture, PCCs are typically connected to a control system which in turn is connected to field instrumentation. PCCs with directly (non-network) attached field instrumentation may have additional and more stringent requirements than those discussed in this document.

Business and non-process-control technical computing functions are not normally performed in computers used for process control. If business functions are placed in the same environment with the process control functions, priority must be given to the control requirements.

4.4 Process Control Computer Functions

A process control computer provides several functions in a typical plant control computing environment. Of highest importance in the overall software scheme is the requirement that each portion of software can communicate and understand every other portion contained in the computer. Inside the computer hardware are many software functions that do the actual, user-visible work in the system. At a minimum, these functions would include the following:

a. An interactive, real-time, multiuser, multitasking operating system with priority processing.
b. Collection and storage of process and engineered data.
c. Database storage for the portions of the distributed global database that this computer owns.
d. Database support and interfaces for the data this computer holds and to the global data in other processors.
e. Execution of processor-monitoring and control algorithms.
f. Execution of advanced control and information-building programs.
g. Most of the security facilities for getting in and out of this computer.
h. Communication services for other data interfaces and networks.
i. Tools for implementing high-level application programs.
j. Man-machine interfaces including display drivers, graphics packages, and report writers.
k. Word processors (editors) to change advanced control programs.

The process control computing environment includes many advanced control applications, production scheduling, inventory management, product blending, and other higher-level optimization control schemes, along with the normal software development functions. These are referred to as *application packages*. Their functions will not be covered by these requirements, but their data-needs will be covered.

Safety shutdown systems should not be part of the PCC system without following OSHA and appropriate process safety management standards, procedures, and documents.

4.5 Performance Requirements

4.5.1 PERFORMANCE OF THE PROCESS CONTROL COMPUTING ENVIRONMENT

Performance of the system is defined in the following areas:

a. Control information processing.
b. Terminal response.
c. Data acquisition.

COPYRIGHT 2002; American Petroleum Institute

Document provided by IHS Licensee=Sincor Venezuela/5934214100, User=, 08/13/2002 12:13:45 MDT Questions or comments about this message: please call the Document Policy Management Group at 1-800-451-1584.

4.5.2 CONTROL INFORMATION PROCESSING

Anticipated normal user requirements for the amounts of data to be processed transfers across networks, and the speeds of response for each type of user are delineated in the sections below.

4.5.2.1 Control Information From Control Network to Control Network

This type of data is considered to be the most critical to operations and has the strictest performance requirements. Typical projected needs are the following:

a. For each control network with a typical database of 3000 points, there will be approximately 10 percent or 300 points that will be used by other control networks in their control schemes.
b. For each of these points, there would be an average of four parameters needed.
c. Range of schedules for data would be from 15 to 300 seconds.
d. Average transfer rate would be 48 parameters per second.
e. Minimum elapsed time between a control network requesting data and the time it gets the values would be 5 seconds, and the maximum allowed time would be 20 seconds.

4.5.2.2 Control Information From Control Network to PCC

This type of data is considered to be almost as critical to operations and has the following typical performance requirements:

a. For each 3000 point control network, at least 15 percent or 450 points will be used by PCC processors in their control schemes.
b. For each of these points, there would be an average of two parameters needed.
c. Range of schedules for data would be from 60 to 300 seconds.
d. Average transfer rate would be 10 parameters per second, but with bursts of 500 parameters per second needed.
e. Minimum elapsed time between a PCC requesting data and the time it gets the values would be 5 seconds, and the maximum allowed time would be 30 seconds.

There is a *fan in* attribute of the system that must be addressed in the configuration. Control data may flow from all the control networks to all the PCCs. Total throughput to a PCC is a function of the amount of data, the number of control networks, and the number of PCCs:

$$\text{Throughput} = \frac{(\text{Data per Network}) \times (\text{Number of Networks})}{(\text{Number of PCCs})}$$

It should be noted that all this control data flows from the control networks on each request or processing of programs from the PCC. None of the lower level control data is held in the PCC database.

4.5.2.3 Control Information From PCC to Control Network

Outputs of the PCC control programs to the control networks average about 30 per program each minute, but these should go out in a burst, thus the required flow rate is 30 per second.

4.5.2.4 Control Information From PCC to PCC

It is anticipated that there will be some data required for control from one PCC to another. This traffic is estimated at about 10 values per second per PCC.

Some historical data will be transferred from PCC to PCC for control. It is estimated that this would require a transfer of 60 values for 20 points in a 5-second window. There will be one request per PCC each minute.

4.5.2.5 Control Information From PCC to Higher-Level Computers

It is anticipated that higher-level computers may need blocks of data periodically. Since this data is typically not time critical and may be averages, totals, and so on, for the previous time period, the data may be supplied at a lower priority than the control functions. This traffic is estimated at 5000 values within 30 seconds at 15-minute intervals.

4.5.3 DISPLAY RESPONSE

Data for display by users on the control networks and on the plant network will be the heaviest usage of communications and data in the system.

4.5.3.1 Control Network Users

Control network display of PCC data will use a small number of point parameter values, lots of history, some records, and infrequently an entire file. Response time is the most important factor; it should not take longer than the following:

a. Five seconds to see point parameter data.
b. Ten seconds to see 500 historical values, or equivalent size records and files.

Control console operators will make few changes to process control computer global data. One record per minute may be updated on average. All operator changes must be posted in no more than 5 seconds.

4.5.3.2 Plant Network Users

Data required for PCC terminal display will be heavy due to the anticipated large number of users. Although each user will call for new data relatively infrequently, for example, with 50 terminals connected, the average demand will be

COPYRIGHT 2002; American Petroleum Institute

Document provided by IHS Licensee=Sincor Venezuela/5934214100, User=, 08/13/2002 12:13:45 MDT Questions or comments about this message: please call the Document Policy Management Group at 1-800-451-1584.

API RP*554 95 ■ 0732290 0549592 970 ■

high for fresh data. Response time shall be 15 seconds or less, independent of the number of terminals.

4.5.4 DATA ACQUISITION

4.5.4.1 Data for Higher-Level Application Packages

The PCC functions described in Section 4.4 will need large bursts of data on a periodic basis for their calculations. Data flows of 1000 values per application, within a 30-second time frame, shall be provided for.

4.5.4.2 Historical Data Access

Requests for historical data can be partitioned into three main areas: access of current data to create long-term history in the PCC machine, access to portions of the history data for reports and storage, and ad-hoc requests for special files of history.

Projected needs in each of these areas are as follows:

a. *Current data access*: The most information a user will require is for all 3000 points' process variables (PVs) on a control network to be transferred once a minute. This would equate to 50 values per second per control network.
b. *Historical data*: Some users will want to transfer the history collected by the local system for long-term storage and archival. If 6-minute averages are transferred once per hour, then the total values would be 30,000 per control network, and the average rate would be 50 different values per second (transfer in 10 minutes elapsed time).
c. *Special history files*: There are some special history files that will occasionally require access. Most notable of these are the sequence-of-events files that store plant disturbances and environmental data. A typical request would be for 100 values from one file in a 5-second burst.

4.5.4.3 Data Access for Reports

Access to data is required for report generation for operations, maintenance, engineering, and management. It is anticipated that the normal plant requirement for point and historical data will be the following:

a. An average of 100 reports per hour with some bursts of 300 reports in an hour, 3 times per day.
b. Each report can contain 300 parameters or 600 history values.

In addition there will be reports of general record data. Total plant requirements for this type of reporting will be as follows:

a. Average of 300 reports per hour.
b. Each report can contain 10 records of 40 fields.

4.5.5 CONNECTIVITY BETWEEN PLANT NETWORKS

Performance will normally be dictated by the communication speed available between networks. At best, the inter-plant transfers would be no faster than local transfers of data and information.

4.5.6 POTENTIAL LIMITATIONS IN THE ARCHITECTURE

Performance will depend on the accumulation of time delay through the complete architecture, the efficiency of each node, and the potential size of the data dictionaries. Also impacting performance are the other tasks the PCC processors are performing. Priorities between the requests from external PCCs and control networks and the requests originating in this PCC to its portion of the global database need to be resolved. Exception reporting can improve communications performance between computers.

4.6 Network Requirements

4.6.1 NETWORK ARCHITECTURE

The primary structure for operating plant information and control systems should be an integrated, multilevel local area network (LAN) architecture.

This architecture must be capable of handling plant level computing and control applications. It must also be capable of integrating the unit level and corporate level data and computing applications.

Data flows (frequency and amount) are consistent with the level of control involved; in other words, seconds and fields at control center level, minutes and records at the plant level.

The distributed nature of the network will require interconnection of computers from multiple vendors, but with the goal that data and information exchange will flow smoothly with a minimum of customization. Digital computers exist at all network levels in the architecture. These requirements deal primarily with the level 3 plant networks.

The basic structure of interconnected multilevel networks is shown in Figure 6. The backbone of this system is the plant network.

4.6.1.1 Network Proper

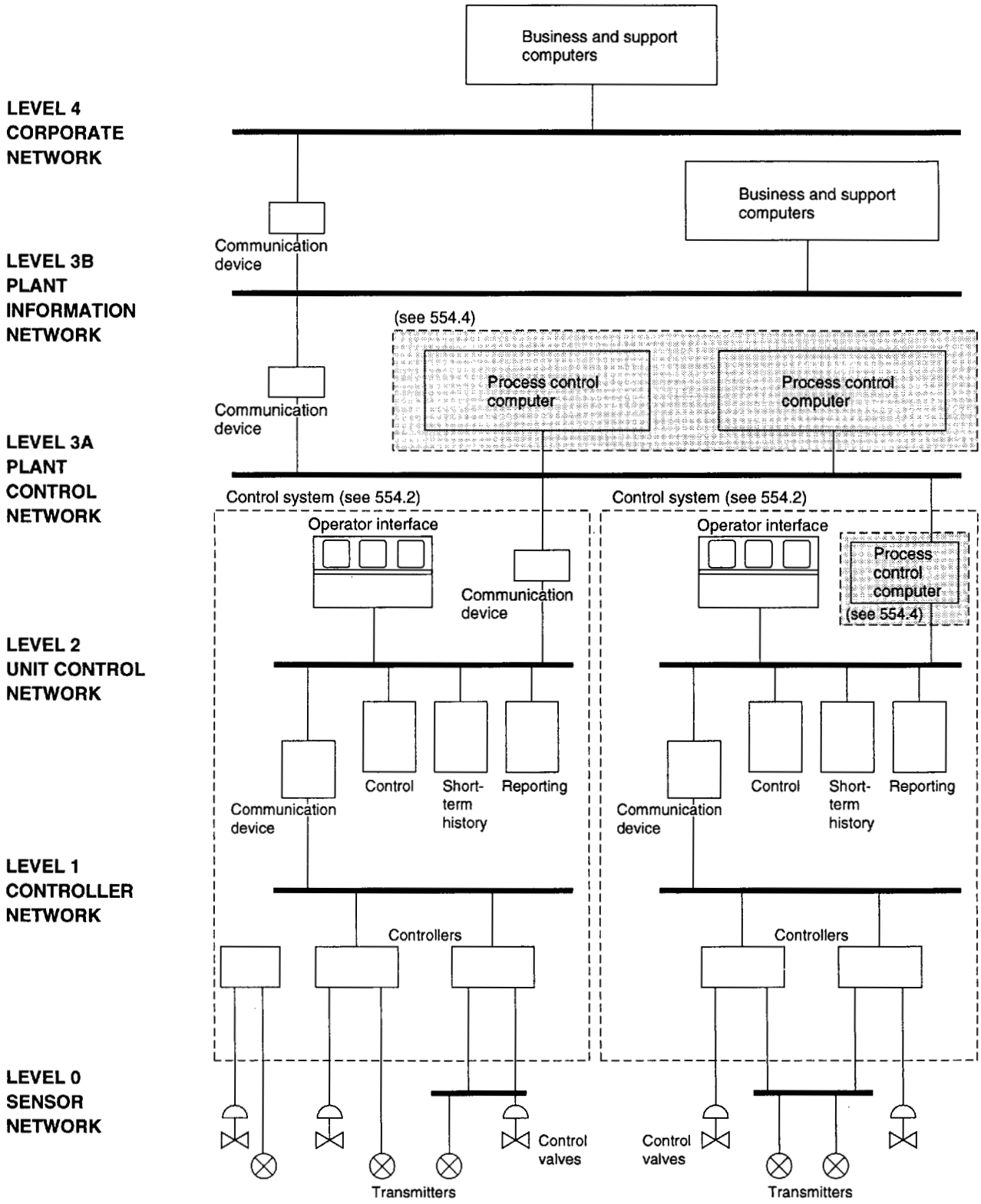
The base component of the plant network is the communication path. Inside the confines of a plant, this path should consist of a broadband network operating in the 10 to 100 megabaud range. Standard coaxial cables or fiber optics should be used as the physical communication path, depending on the environmental requirements and throughput desired. The plant network should be capable of operating at distances from 10 to 25 kilometers. Beyond the boundaries of a plant, it must be possible to communicate data to a corporate network.

4.6.1.2 Network Interfaces

Interfaces must be provided among the control system networks, the plant network, and the corporate network. Gateways, bridges, routers, and repeaters are typical inter-

COPYRIGHT 2002; American Petroleum Institute

Document provided by IHS Licensee=Sincor Venezuela/5934214100, User=, 08/13/2002 12:13:45 MDT Questions or comments about this message: please call the Document Policy Management Group at 1-800-451-1584.



Note: 554.2 is equivalent to Section 2 of this RP.
554.4 is equivalent to Section 4 of this RP.

Figure 6—Functional Process Instrumentation, Control, and Information Network Architecture, View B

COPYRIGHT 2002; American Petroleum Institute

Document provided by IHS Licensee=Sincor Venezuela/5934214100, User=, 08/13/2002 12:13:45 MDT Questions or comments about this message: please call the Document Policy Management Group at 1-800-451-1584.

API RP*554 95 ■ 0732290 0549594 743 ■

face devices required for interfacing between devices and networks. These interfaces take care of network operation, clocking, transmissions and retries, error checking, and so forth.

Security, capacity, and geographical considerations may dictate segmenting the plant network into multiple sections. Filtering bridges and/or routers may be used to segment the plant network if required.

All interface devices should support the Management Information Block (MIB) structure specified by SNMP (Simple Network Management Protocol) and CMIP/CMIS (Complex Management Information Protocol/Services) for OSI (Open Systems Interconnect) to facilitate the task of network management. CMIP is the recommended direction.

4.6.2 NETWORK PROTOCOLS

Network protocols at each of the top three levels will progress over time. Major types of protocols and media are listed in Table 3.

4.7 Hardware Requirements

A PCC consists of many hardware components plus appropriate software that, when properly selected and assembled, forms a system with the functionalities desired by the user. This section will review the major parts of the PCC system and provide some guidance on system selection.

4.7.1 GENERAL DESIGN CONSIDERATIONS

There are several general design parameters for a PCC system that should be considered prior to sizing the system. These parameters depend on both the current and future expected use of the PCC system.

4.7.1.1 System Availability and Reliability

Systems used for process control should be available for a minimum on-line processing factor of 99.6 percent, including scheduled system maintenance. This service factor should be for the anticipated life cycle of the system. A PCC system should feature automatic reboot. Battery power backup is recommended for critical applications.

Requirements for recovery time from outages vary depending on application and the use of a distributed control system for regulatory control. System recovery times of 1 to 2 hours are acceptable.

A PCC system should provide for automated backup of critical database files to tape or shadowed disk drives.

4.7.1.2 Modularity and Expandability of Design

A PCC system should be easily networked to other computers (PCC and management information systems) as well as to a variety of distributed control systems. This will enable easy expansion without replacement of the existing system as processing requirements grow.

4.7.1.3 System Obsolescence

Since computing technology is advancing rapidly, care must be taken to insure that any system will not become obsolete, therefore becoming a maintenance problem within a few years.

The system vendor should be able to show evidence of upgrade compatibility of older systems as new technologies are made available. Before loading new operating-system software, make sure that it will support the hardware, advanced-control application software, and interface drivers.

4.7.1.4 Control System Interfaces

A PCC system shall be chosen that supports all desired regulatory control system interface connections. Special attention should be paid to selected DCS interfaces. If process analyzers, electronic board-mounted controllers, programmable logic controllers, and so on, of interest cannot be connected to the DCS, then they must be able to interface directly into the process computing environment.

Device interface reliability should be a minimum of 99.9 percent. Hardware connections should match the chosen network protocols (see 4.6 and Table 3). If proven interfaces do not currently exist, care should be taken in developing new interface drivers.

Table 3—Major Types of Protocols and Media

Network Layer	Protocols	Link Layer	Physical Media
Unit Control Level 2	Proprietary OSI	Proprietary	DCS Network
Plant Network Level 3	Proprietary TCPIP/IP OSI[a]	Token Passing IEEE 802.3 EThernet[a] ANSI ASC X3T9.5 FDDI[a]	Twisted Pair Coax Cable Fiber Optics
Corporate Level 4	Proprietary TCP/IP OSI[a]	—	

[a]Recommended directions

COPYRIGHT 2002; American Petroleum Institute

Document provided by IHS Licensee=Sincor Venezuela/5934214100, User=, 08/13/2002 12:13:45 MDT Questions or comments about this message: please call the Document Policy Management Group at 1-800-451-1584.

4.7.2 CENTRAL PROCESSING UNIT

The central processing unit (CPU) runs the operating system software that controls all aspects of program execution, provides system security, and manages all system resources. Selection of a CPU depends primarily on the user's intended application requirements for memory, disk space, and peripherals.

4.7.2.1 CPU Sizing

The CPU must be sized to insure that it provides adequate performance for the user's application. An approximate way to do this is to add up the MIPS (millions of instructions per second) required by each of the following:

a. All concurrent logged-on users.
b. High-frequency, scheduled data transfers.
c. High-frequency, scheduled applications programs.

These requirements are highly dependent upon the hardware platform and the specific applications. This information may be available from the computer system manufacturer and/or the application software vendors. Benchmark testing for throughput is highly recommended as a performance measure.

It is recommended that the CPU be sized for 50 percent loading to allow for additional routine use (for example, for program development).

4.7.2.2 Other CPU Features

Auxiliary power is recommended for CPUs for all PCCs. This can be achieved by either a UPS or by a main memory battery backup (see 4.16.1.4).

A hardware floating point co-processor is recommended. Parallel or array processing CPUs may be appropriate for some high-performance process control applications.

4.7.3 MAIN MEMORY

The amount of Main Memory [or Random Access Memory, (RAM)] is highly dependent on the computer, the user applications, and the way that the computer will be used. Factors that affect main memory requirements include the users, the process control applications, and the caching of data.

4.7.3.1 Main Memory Sizing

The general approach to memory (for example, RAM) sizing is to determine and sum up the main memory requirements of the following:

a. The operating system.
b. The user software.
c. The process control applications.
d. The data acquisition/historization application.
e. The amount for each concurrent logged-on user.

These requirements may be available from the computer manufacturer and/or the applications software vendors. It is recommended that memory of the system be at least the above requirement plus 25 percent spare capacity. In addition, it is recommended that memory can be expanded in the future to double the above requirement.

4.7.3.2 Process Control Applications

The memory should be sized so that all high-frequency process control applications can be resident in memory simultaneously, plus enough memory to minimize the swapping of files to disk.

4.7.4 SYSTEM CLOCK

Each CPU must have a real-time system clock. An accurate system clock is necessary to provide program scheduling functions and to provide timestamping for process data. The capability to synchronize time with other computers and with the lower-level control system should be provided to insure consistent process data timestamps. The clock should be independent of voltage or frequency fluctuations.

4.7.5 BULK STORAGE DEVICES

Bulk storage devices supplement main memory and can contain programs and data that can be loaded into main memory as needed. They are also used to store data for archival purposes. Bulk devices can be fixed or removable, should contain sufficient caching to not impede CPU performance, and should include features that improve data integrity (for example, read after write).

4.7.5.1 Fixed Bulk Storage Devices

Fixed bulk storage devices are usually hard disk drives. High-performance drives are recommended for frequently accessed data (system disk, process control applications, recent historical archive). Larger, slower-access disks are acceptable for files that are accessed less frequently (for example, archived data more than 1 week old).

4.7.5.2 Removable Bulk Storage Devices

Recommended types of removable bulk storage devices, used for disk backup and off-line data archiving, are cartridge streaming tape and optical disks. Other types of removable storage are available for smaller amounts of data, including removable hard disk drives, floppy drives, and Bernoulli drives.

4.7.5.3 Bulk Storage Device Configuration

The following is the recommended bulk storage configuration:

a. One drive for system (fixed, high-performance disk).
b. One drive for control applications (fixed, high-performance disk).

COPYRIGHT 2002; American Petroleum Institute

Document provided by IHS Licensee=Sincor Venezuela/5934214100, User=, 08/13/2002 12:13:45 MDT Questions or comments about this message: please call the Document Policy Management Group at 1-800-451-1584.

c. One drive for recent archive (fixed, high-performance disk).
d. One drive for archiving (removable disk).

This list should be tailored to the needs of the specific application.

4.7.5.4 Disk Shadowing

Additional security can be provided for data stored on bulk storage by providing a disk shadowing system. In the extreme, this may take the form of providing one-to-one redundancy for each disk, where every piece of data is written to two disks. Or, a single shadow disk can be provided for multiple disks. When system software predicts disk failure based upon recoverable errors, the shadow disk will automatically be written to and will take over operation from the bad disk.

The level of disk shadowing will depend upon the individual application and upon how critical the data is on the disks. Disk shadowing is recommended for the system disk and for critical data.

4.7.5.5 Bulk Storage Sizing

Bulk storage should be provided to support each of the following:

a. System software.
b. Data archiving (application and archived data storage).
c. Process control applications.
d. User support.
e. Disk shadowing.

Storage requirements for system software should be available from the computer system manufacturer. Storage requirements for archived data will depend upon whether data compression is used. For each point collected, the value, the status, and the timestamp are typically stored. Recommended storage sizing is a minimum of 6-minute averages of process data for every process value on all networks for total storage of 1 year on-line.

Storage requirements for process control applications will be highly dependent upon the quantity and type of application. Information may be available from the software applications vendor.

User support storage requirements include storage space for program development, scratch, and so forth. Space must also be provided for disk shadowing functions if used.

It is recommended that at least twice the amount of required storage as determined above be provided in this environment.

4.7.5.6 Removable Bulk Storage Sizing

It is recommended that a minimum of two removable bulk storage devices be provided. This includes one for data archiving functions and one for data retrieval. The removable device should be sized as large as the largest fixed device, with sufficient capacity to hold data for one-half year.

4.8 Peripherals

Peripherals must be provided to allow the computer system to communicate to users and to other systems.

4.8.1 SYSTEM TERMINAL

A system terminal should be provided as recommended by the computer manufacturer.

4.8.2 OPERATOR STATION

The recommended means for process operators to communicate with the PCC is through their process control system workstation (normally the distributed control system CRT). This approach allows for a consistent method of data presentation to the operator and minimizes the potential for operator confusion. If this approach is not possible, a separate computer station should be provided for the operator.

4.8.3 ENGINEERING STATIONS

A minimum of one engineering station should be provided, suitable for programming, editing, maintenance, and other functions required to support the system. This station should support color graphics.

4.8.4 PRINTERS

It is recommended that the PCC be supplied with at least one type of printer peripheral. The types of printer selected, line printer, laser, or dot matrix, will depend on the user's requirements. All printer resources should be connected to the network to allow sharing of resources.

4.9 Non-Network Communications Ports

Communications ports, serial and parallel, synchronous and asynchronous, are available to direct-connect peripherals to the computer.

Communications ports may also be used to allow communications via modems to other systems and remote computers. To insure system security, access to the PCC through shared communications lines (for example, telephone lines) should be closely controlled and restricted.

Communication ports need to be designed to handle project requirements.

4.10 Software Requirements

4.10.1 ORGANIZATION OF PROCESS COMPUTER SOFTWARE

Process Computer Software includes all the software that is contained in the Process Control Computer (PCC). Since

COPYRIGHT 2002; American Petroleum Institute

Document provided by IHS Licensee=Sincor Venezuela/5934214100, User=, 08/13/2002 12:13:45 MDT Questions or comments about this message: please call the Document Policy Management Group at 1-800-451-1584.

API RP*554 95 ■ 0732290 0549597 452 ■

the PCC itself may consist of several physical devices, the PCC and its software need to be addressed as an integrated whole with the overall corporate, plant, and control networks. The user, or system integrator, is responsible for software that achieves the operability without duplicating functions or data.

The conceptual layout for the PCC memory is shown in Figure 7, PCC Memory Layout. The heart of any computer is its native operating system, which is depicted at the center of the circle. The four main PCC activities—device drivers, data acquisition and history, user software, and process control applications—are shown in each quadrant. Since the concept of depicting systems as circles implies that there is communication only toward the center and back out, a shared program library area is shown just outside the operating system. The programs in this library are supplied by the various vendors for programmatic access to their packages. These routines also help to implement standard methodology and machine and operating system independence.

The shared program library capability is the key to provide programmatic access to third party products and to ensure interoperability with the overall corporate and plant networks. This library should contain tool kits provided by and maintained by each vendor for programmatically accessing their systems. This tool kit approach eliminates the need for users to know the internals of each vendor's products. This tool kit technique of program calls, as opposed to file transfers, both speeds the data transfer and frees multiple parties from having to agree on file structures.

The following list provides examples of steps to increase development productivity, speed user acceptance and application development, and decrease maintenance costs and delays:

a. The shared program library should contain appropriate functions for all types of displays and for data distribution across the various networks.
b. Display and logging should be processed through a language resource. The language resource not only provides a convenient method of switching from one language to another, but also provides a convenient source for all instructions and error messages that can be sent to the various users.
c. A windowing environment uses consistent user-interface standards and routines to control the screen and its behavior. This means that the user has to know only one method of interaction with the PCC and not a unique method for each application and that the system administrator has to maintain only one set of user interface routines.
d. Calculation-intensive applications should be capable of being executed in distributed computers, if necessary.
e. All software should use generic operating system calls to facilitate operation on a variety of hardware.
f. Maximum use of generic operating system calls and existing software should be made, whenever possible. For instance, process control applications would use the data acquisition/historian software to get and send data to the control system.

4.10.2 OPERATING SYSTEM

The operating system performs many functions. Typical functions include the following:

a. An interactive, real-time, multiuser, multitasking environment with priority and interrupt scheduling to support the activities depicted in Figure 7.
b. Security for access to devices it controls and for access to and from other networks.
c. Queue processing by priority time slice, time and event scheduling, and priority interrupt control.
d. Redundancy of the CPU (fault tolerance) and of hard disks (mirroring, shadowing, and so on), if desirable.
e. Data storage management (4.7.5).
f. Peripheral control (4.8) and non-network communications (4.9).
g. Virtual and real-memory management.
h. Real-time clock and time synchronization with other systems. There should be one master time stamp within the entire network of computers, and the systems should automatically synchronize with each other.
i. Display management (4.5.3).
j. Plant network communications (4.6).
k. Control network communications (4.10.7).

Desirable functions include the following:

a. Imminent power failure response. When the UPS serving the operating system notifies the operating system that it has switched to auxiliary power, the operating system should notify users and connected systems that it is likely to shut down within a specified time period, unless it receives additional power. Optionally, if additional power is not supplied, then the operating system may be configured to conduct an orderly shutdown.
b. Data recovery after a crash. Data that was in transition prior to shutdown should not be lost.
c. Each site should follow a backup master plan that provides for data recovery from total data loss at any time. Such a plan should not require any applications to cease functioning while the data is backed up.
d. Application compilers and modular integration to minimize functionality duplication due to future use of distributed and parallel processing.

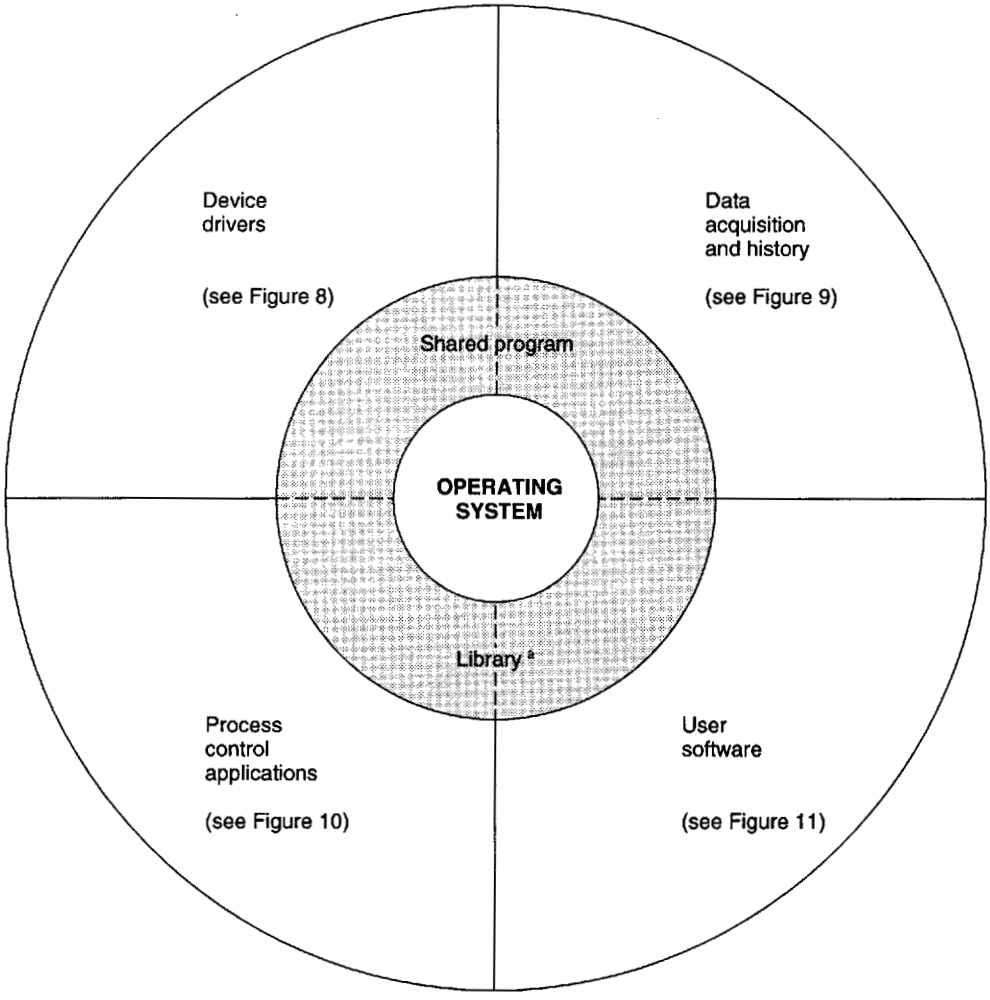
Overall system architecture standards should be set to provide a means for measuring the interoperability of possible operating systems.

4.10.3 PCC APPLICATIONS AND INTERFACES

All process control programs are to be operated on computers specifically reserved for that purpose to minimize

COPYRIGHT 2002; American Petroleum Institute

Document provided by IHS Licensee=Sincor Venezuela/5934214100, User=, 08/13/2002 12:13:45 MDT Questions or comments about this message: please call the Document Policy Management Group at 1-800-451-1584.



Note: This PCC memory layout is as presented in Section 4.

[a] To implement a standard methodology including machine and operating system independence, a shared library provides the programs that link each quadrant:

- Network communications
- Graphics
- Displays
- Reports
- Language
- Database structure
- Database access
- Application specific
- User specific

Figure 7—PCC Memory Layout

the effects of other programs or system administration procedures affecting the process control operation. Generally, these computers will be dedicated to the process, and they may pass data upwards to plant information computers, but that is only a secondary task.

As shown in Figure 7, the PCC has four major activities to perform. These activities are to communicate with other devices (of any type); to acquire, historize, and serve data; to control processes; and to provide a user application development platform.

4.10.3.1 Device Drivers

Only one set of device drivers should be provided for each device type. As shown in Figure 8, PCC device drivers include these:

a. The corporate, plant and control networks. This area addresses the transport, network, data link, and physical layers of the OSI (open system interface) model, layers 1 through 5.

b. All bulk storage devices, disks, tapes, CD (cartridge disk), and so forth.

COPYRIGHT 2002; American Petroleum Institute

Document provided by IHS Licensee=Sincor Venezuela/5934214100, User=, 08/13/2002 12:13:45 MDT Questions or comments about this message: please call the Document Policy Management Group at 1-800-451-1584.

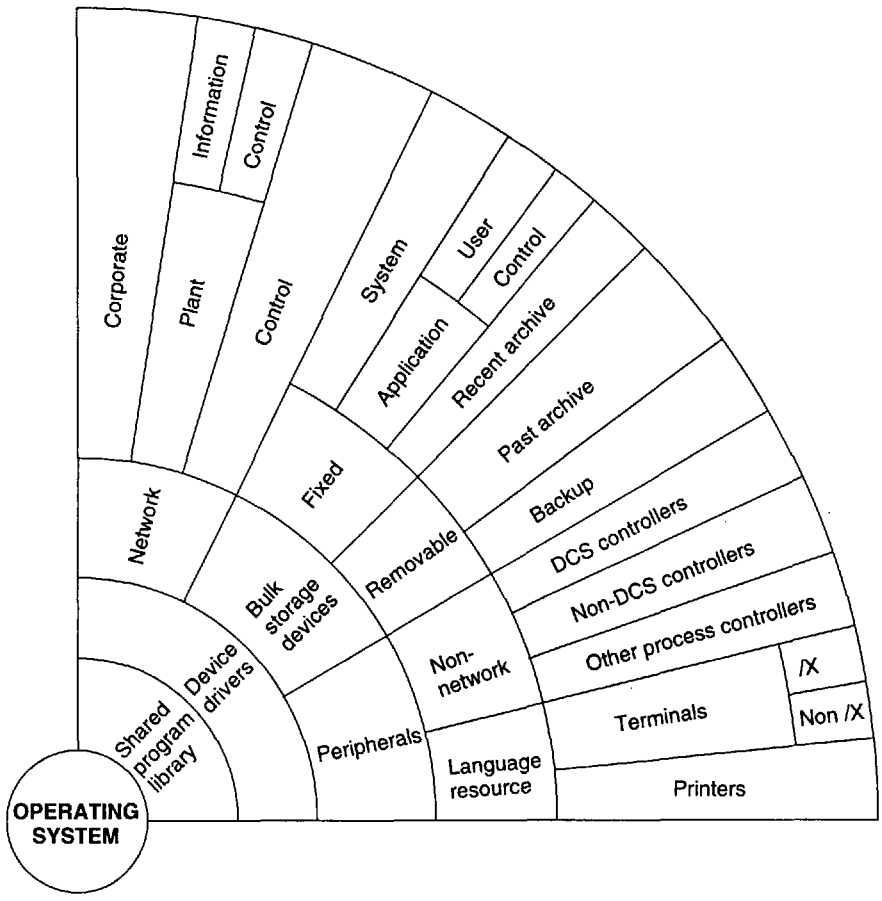


Figure 8—PCC Device Drivers

c. All peripherals, any control system or subsystem that is not networked, would be interfaced in this category. The networked devices, application, and presentation communication layers of networked devices would be addressed here. Also, any terminals, printers, and the like, would be interfaced here. This concept facilitates the use of a language resource to display the information in the language of the user's choice, independent of any other user.

4.10.3.2 PCC Data Acquisition and History

The PCC is usually responsible for acquiring data from all applicable data sources, historizing that data, and providing (serving) the data to anyone or anything with proper security that requests it (see Figure 9). Concentrating data acquisition and serving frees other programs from having to duplicate these functions. The types of data are discussed in detail elsewhere in this standard. For this overview, one needs to understand the following:

a. Data management includes the acquisition and serving of point data, current and time series, general data, time stamped events, text, and so forth. In each case, current data is uniquely handled and may be bi-directional with the connected devices. Time series point data may be aggregated or compressed prior to storing. General data is not compressed or aggregated prior to storage.

b. Data access routines to the current or historical data need to provide for retrieval in a variety of time periods and forms. For example, average, minimum, or maximum point data may be requested for a given time period, or general data may be requested in the order of the time stamp.

c. Data transfer may be across the corporate, plant, or control networks or within the same physical machine. In any case, proper security needs to be enforced and the desired aggregations performed before the transfer.

In short, the data historian should provide bi-directional, interactive data acquisition and historization applications with data access for control applications, trending, analysis, and report writing. This application should have programmatic calls for current values, for historical values, and for events. The historical value(s) calls should provide for specifying the time period and interval of the aggregation method, for example, hourly averages, minimum and

COPYRIGHT 2002; American Petroleum Institute

Document provided by IHS Licensee=Sincor Venezuela/5934214100, User=, 08/13/2002 12:13:45 MDT Questions or comments about this message: please call the Document Policy Management Group at 1-800-451-1584.

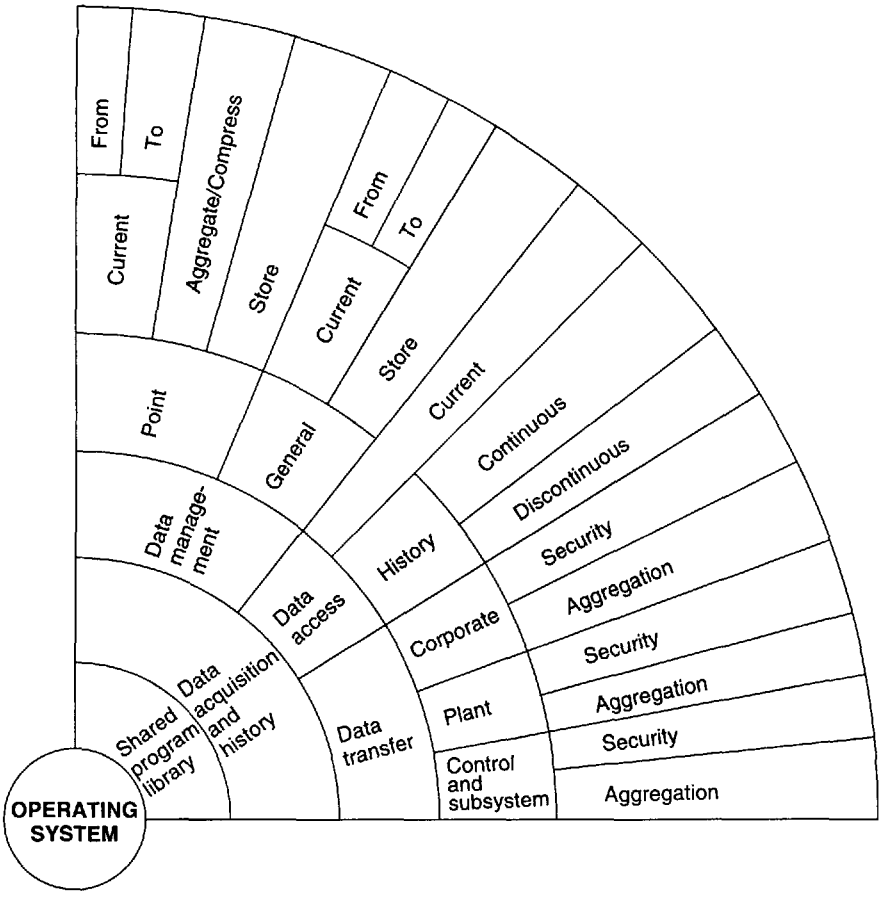


Figure 9—PCC Data Acquisition and History

maximum. The event lists should provide for specifying the time period and a filter to retrieve only the events of interest.

4.10.3.3 PCC Process Control Applications

In this context, PCC process control applications (see Figure 10) run continuously to control and optimize the connected processes. The applications may be vendor- or user-developed packages or custom implementations. Typical generic applications include the following:

4.10.3.3.1 Pass balancing, internal reflux control and calculations, ratio control, and cooler trim control are included. (The traditional applications that most distributed control systems can also perform.)

4.10.3.3.2 Mathematical modeling and control, statistical process control, matrix control equation-solving methods, composition analyzer modeling and replacement, batch modeling and controls, unit optimization and plant optimization modeling and control are also included.

4.10.3.3.3 Some applications outside the processing units include these: blend ratio and property controls, tank farm and inventory storage and management systems, tank movement programs, pumping lineups, and leak detection programs.

4.10.3.4 PCC User Software

PCC user software (see Figure 11) includes all the tools to develop, test, diagnose, and run individual applications.

4.10.3.4.1 Software development is limited to only those personnel who have appropriate security clearence. Therefore, all programs that are used for application development should require a special security level. These programs include the following:

a. *Compilers and linkers*: The PCC vendor should offer compilers and linkers for C, FORTRAN, and Pascal as well as facilities for fourth-generation language toolkits. The compilers should not degrade system performance and should run and permit linking and execution while real-time applications are executing. Programs compiled or linked on one version of the same computer family should be executable or linkable on another version of the same family.

The compilers should provide debugging and tracing

COPYRIGHT 2002; American Petroleum Institute

Document provided by IHS Licensee=Sincor Venezuela/5934214100, User=, 08/13/2002 12:13:45 MDT Questions or comments about this message: please call the Document Policy Management Group at 1-800-451-1584.

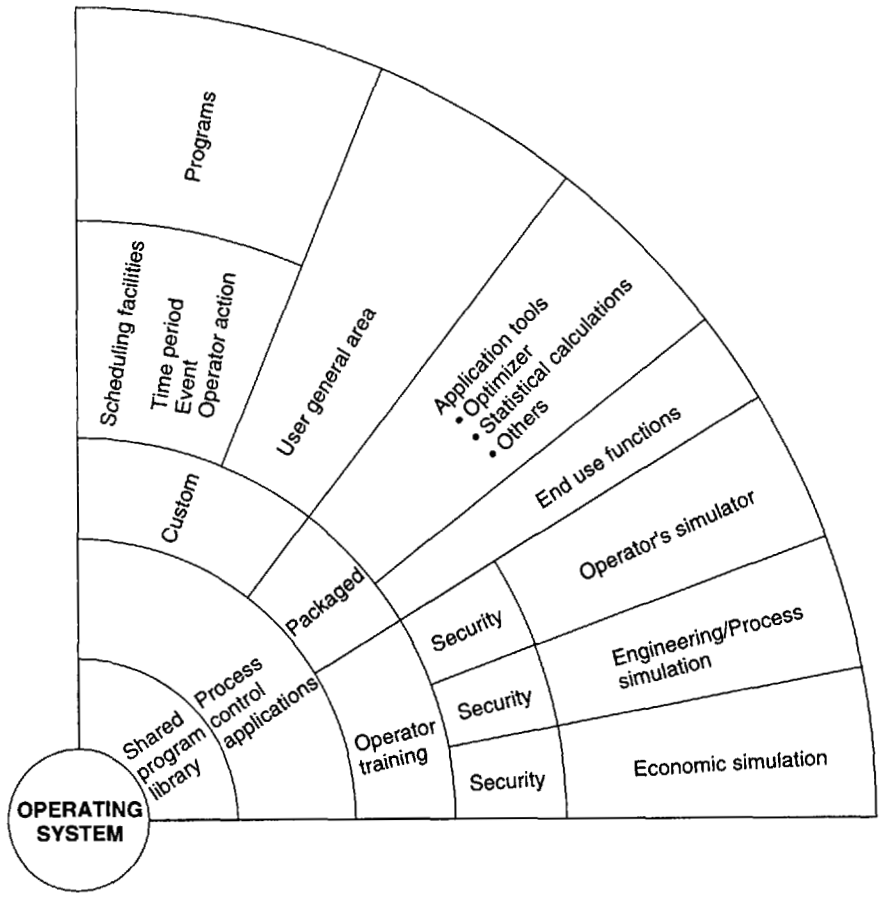


Figure 10—PCC Process Control Applications

functions, as well as program analyzers to aid in debugging and for efficient code development.

A decompiler would be helpful for troubleshooting and code validation.

b. *Support routines*: The support routines should include a site specific library for common calculations, and so forth. Tools that provide for screen and report development and management would expedite consistent code development.

Linkage of compiled code from a variety of compilers should provide for dynamic access to the shared libraries. Such dynamic access ensures the consistency of all calculations and minimizes hard disk storage requirements.

c. *Diagnostics*: Since real-time programming is by definition complex, imbedded diagnostic routines facilitate verification of all options within the code.

4.10.3.4.2 *Ancillary programs*: All programs that are not for control, but may be used by the operators or engineers working on the PCC should be grouped together under this heading. The use of the PCC for ancillary programs is not a recommended practice and is only mentioned for those users that have no other choice. Examples include the following:

a. *Word processing*: Although word processing on the PCC is not a requirement, a good ASCII file editor should be included or purchased separately. Editors that integrate with the programming standards, libraries, and release control procedures facilitate program development. In fact, the editor's help system should include context sensitive help for the program libraries that developers use. Help for windowing-environment development tools, object-oriented procedures, and client/server application libraries are a few of the context sensitive help systems that should be integrated with the program development editor.

b. *Electronic mail*: It is not recommended, but if the PCC system is the "home" address for the system developers or any other members of the plant network user community, then an electronic mail groupware product that interoperates with the corporate standard product is recommended. At the very least, the electronic mail package should include the ability to edit and spell check the document before distribution, the ability to request the equivalent of a return receipt, and so forth.

The PCC should facilitate the utilization of the corporate standard electronic mail system by the operator.

COPYRIGHT 2002; American Petroleum Institute

Document provided by IHS Licensee=Sincor Venezuela/5934214100, User=, 08/13/2002 12:13:45 MDT Questions or comments about this message: please call the Document Policy Management Group at 1-800-451-1584.

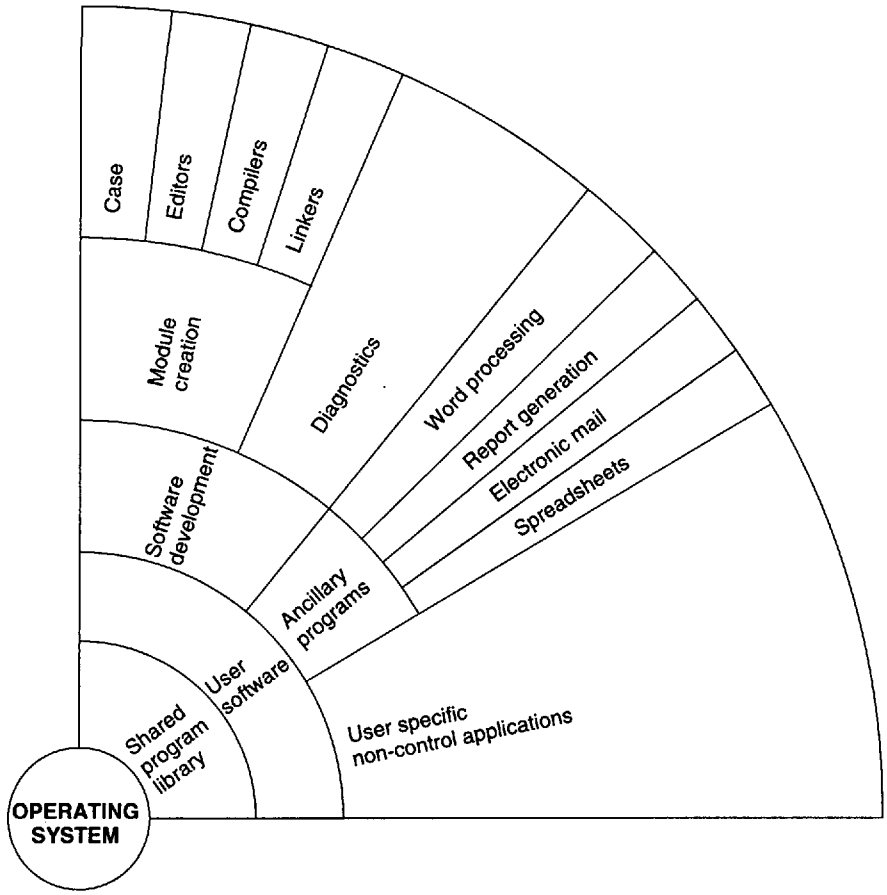


Figure 11—PCC User Software

c. *Other programs*: Other programs might include spreadsheets, and so forth, that are not dependent upon real-time data.

4.10.3.4.3 *User specific applications*: Users often have unique programs that they run periodically. This category provides for their secure storage and application. Examples could include off-line controller tuning, control application performance summary, and the like.

4.10.4 DATA MANAGEMENT AND THE GLOBAL DATABASE

Inside each processor of the processing computing environment is that portion of the global database that belongs to this processor and the data manager that keeps track of data and its access.

Following is a description of each of the main types of data that would be stored and accessible via global data support.

4.10.4.1 Point Record Structures

It is required that there be a point records database maintained in the PCC, similar to the *point* records on the control networks and process connected networks.

These points must be stored as a *point name* with all attendant *parameters* via the point name. There should be a minimum fixed set of parameters for all points, followed by custom named parameters relative to the type of data held by that point.

Examples of the parameters would be the following:

a. Fixed
   1. Point name.
   2. Description.
   3. Engineering.

b. Custom
   1. Analyzer component 1.
   2. Analyzer component 2.
   3. Analyzer component 3.

Currently, it is envisioned that there would be no configured processing on these points. All data would be stored into the records by their PCC or other authorized nodes on the network. Control is executed by application programs and the results stored into the database.

4.10.4.2 General Record Structure

There must be a general records structure in the database.

COPYRIGHT 2002; American Petroleum Institute

Document provided by IHS Licensee=Sincor Venezuela/5934214100, User=, 08/13/2002 12:13:45 MDT Questions or comments about this message: please call the Document Policy Management Group at 1-800-451-1584.

This structure is used to develop special records for specific application needs. The user must be able to define the names of the fields in these records, allowable formats, ranges, and so forth.

An example usage of this facility would be constructing an emissions testing form for the operations department. (See Figure 12.)

Fugitive Emissions Testing Form_____
Test Number_____
Date _____
Emissions Source Tag Number _____
Point ID _____
Testor's Name _____
Test Instrument ID _____
Time of Reading_____
Reading Value _____
Units_____

Figure12—Example of a Record

This portion of the database would be accessed by gaining authorization into the general area (for example, Fugitive Emissions Testing) and then getting the record and fields desired.

4.10.4.3 Continuous History Database

There is a requirement for a long-term historical database for continuous data. Inputs to this database are any point.parameter combinations in the global database. On-line data for each parameter historized could include the following as a minimum:

a. Six-minute averages for at least 2 years.
b. Hourly averages for at least 2 years.
c. Shift, daily, weekly, monthly averages for at least 10 years.

In addition to the actual history value for each time increment, other data would be the following:

a Number of valid samples in the average.
b. Highest and lowest values during the time period.
c. Other statistical values found to be necessary.

Data compression techniques could be used to reduce the amount of bulk storage required. If data compression is used, consideration should be given to techniques that reproduce the original form of the data. Accessing of the historical data would be by specifying the following:

a. Plant Network. Point Name. Parameter.
b. Starting date and time / Ending date and time.
c. Type of history data desired (for example, averages, ranges, statistical parameters).

This long-term historical database would be in addition to any short-term history kept by the control or process networks.

4.10.4.4 Discontinuous Historical Database

Another type of historical data required is for operations or groups of data that are discontinuous by nature. Examples of the types of applications are the following:

a. All data pertaining to a batch of gasoline blend.
b. A snapshot of operating conditions on the catalytic cracking unit during a particularly good run.
c. The series of actions leading to shutdown of a compressor.
d. The sequence of events just before and after a turbine failure.

Data contained in the fields of these records could include numerical values, journal entries, operator actions, system status, and so forth.

The user would define the criteria for collection of a data set, and what data the set was to contain. In most cases, the PCC would be responsible for collecting the information when the criterion was met. In some cases, other devices could collect the set and push it to the host for storage.

Retrieval of the whole record of the set, specific portions of a set, and specific portions of several sets of the same type could be provided.

4.10.4.5 Relational Characteristics of the Database

All areas of the distributed global database in the PCC should be accessible by relational techniques.

All the types of queries and searches common to relational databases must be supported.

4.10.4.6 Data Management Functions

The data manager inside the PCC has several primary functions:

a. Keeping track of where data is located inside this machine.
b. Knowing where data is located outside this machine.
c. Governing access and security of the data.
d. Marking any modified data.
e. Logging where and when changes were made.

These routines will facilitate compliance with OSHA 29 *CFR* 1910.119.

4.10.4.6.1 *Data directories*: Resolution of where the data is stored could be accomplished before any calls were made, during the first call, or upon each request. The system should track any changes in the location of data, if it is mapped, to avoid any transmission of erroneous information.

4.10.4.6.2 *Priorities and authorization*: Prioritization of data calls will be necessary for information requested across the plant network. Several levels of priority are required:

COPYRIGHT 2002; American Petroleum Institute

Document provided by IHS Licensee=Sincor Venezuela/5934214100, User=, 08/13/2002 12:13:45 MDT Questions or comments about this message: please call the Document Policy Management Group at 1-800-451-1584.

a. Operator changes have the highest priority.
b. Control programs to get their required information or store results.
c. Requests for display information.
d. Acquisition of data to store in the PCC database.
e. Request for reporting or other low-priority functions.

Stores to the database will require the *enable* flags to be set, the point to be in the correct *mode*, and the user to be at the correct authority level.

4.10.4.7 Data Access to Nodes in the Plant Network Architecture

In concept, any node on the plant network can acquire and store global data to any other plant network node or the modules attached to it. The only restrictions are determining whether the data desired is part of the global database and whether all the required security checks can be passed.

4.10.4.7.1 *Control network data access*: Control network exchange of data can be divided into two main areas: transfer of data from a control network to a PCC and transfer of data from computer to a control network.

PCC data should be accessible to the control network using global calls. Point data must be available for advanced control schemes, operator display, and reporting. Historical data would be used primarily for displays and reports. Record data could be used for control, and for operator interaction at the Control Network level, such as filling out maintenance work requests.

4.10.4.7.2 *PCC processor data access*: At least two types of data access must be supported by the PCC program calls for data, and user terminal calls for data.

Program calls must be available for high-level languages, such as FORTRAN, Pascal, and C. These calls will allow the user to import and export data from his programs using normal subroutine-type functions. The user must be able to get any data, of any type or amount, from the global database. It will be up to the user programmer to insure that there is enough storage capability for his use and that it is of the right types.

4.11 Human Interfacing

4.11.1 INTRODUCTION

The human interface in the process computing environment is a crucial element. It is the key to easy and efficient response by operators and others to the large amount of information available.

Interfaces are typically CRT screens, keyboards and printers that are directly connected to the process computing environment or part of the DCS.

The PCC human interface should have a consistent "look and feel" for all applications, with the flexibility to be configured for use by several classes of users.

Special attention should be made to alarm and emergency situations to help operators recognize the nature of the occurrence and to facilitate the appropriate response.

The goals of the PCC human interface system are as follows:

a. Ease of use.
b. Consistency for users in the environment.
c. Data presentation in easily recognized form.
d. Simple security entry and comprehensive notification of security passage or violation.
e. Facilities for displaying all information, data, drawings, and documents.

4.11.2 USER GROUPS IN THE PROCESS COMPUTING ENVIRONMENT

There are three groups of users:

a. Operators and other frequent users: Other frequent users can include control room supervisors, maintenance personnel, or plant personnel.
b. Process Control Engineers: Engineers configure databases. This group includes the set-up, control, and monitoring applications.
c. Others, any plant personnel needing information, but not on a regular basis:
   1. Maintenance or engineering personnel who are not in volved in the daily operations.
   2. Management or administrative personnel who need information occasionally.

4.11.2.1 Operator Task Analysis

Tasks that the human interface must provide for include the following:

a. Monitor plant status and trends.
b. Handle alarms generated by the PCC.
c. Change control variables such as set-points, controller modes, and other process variables.
d. Start and stop control/monitoring applications, batch processing, and so forth.
e. Record data values reflecting operating and off-line analytical results.
f. Print CRT displays.
g. Monitor control application.
h. Make an inquiry to establish the values of process plant parameters based on logical groupings, displays, process units, or zones.
i. Monitor historical values and analyze reports, logs, and trend charts.
j. Use analytical tools to search for patterns of process plant behavior.
k. Extract historical information for use in analytical environments.

4.11.2.2 Engineer Task Analysis

An *engineer* is defined as the person responsible for

COPYRIGHT 2002; American Petroleum Institute

Document provided by IHS Licensee=Sincor Venezuela/5934214100, User=, 08/13/2002 12:13:45 MDT Questions or comments about this message: please call the Document Policy Management Group at 1-800-451-1584.

configuration, implementation, and maintenance of a data monitoring and control system, including applications implementation. The engineer can perform the same monitoring tasks as listed for the operator and additionally the following:

a. Configure the system database, including these:
   1. Build tags.
   2. Set tag parameter values.
   3. Assign and configure the historical database.
b. Implement control and data monitoring applications, including:
   1. Build sequential control sequences.
   2. Write applications.
   3. Configure continuous control applications.
   4. Determine controller tuning constants.
c. Build CRT screen graphics and reports, including the following:
   1. Build screen backgrounds and dynamic (updating) foregrounds.
   2. Build and schedule reports (This may be an operator function).
d. Monitor system performance.
e. Analyze process information.

4.11.2.3 Other Task Analysis

Since this category includes all other plant personnel, there will be a wide variety of tasks that could be involved. As plant personnel continue to use the system, additional tasks will be defined. The broad range of tasks will include design engineering, hazards analysis, using information to make management decisions, and many others.

4.11.3 USER REQUIREMENTS

4.11.3.1 General User Requirements

The following are general user requirements:

a. PCC system processes, modules, and display functions should be available in the PCC terminal.
b. CRT presentations may be full-graphic displays or partial full-graphics displays, and nongraphics displays.
c. All host system functions must be available for monitoring and control.
d. Multiple windows should be available for monitoring and control.
e. High-resolution color-graphics monitor.
f. Consistent color use determined by user with multiple methods of displaying information (for color-blind person).
g. Context sensitive help.
h. Ergonomically designed panel layout and environment.
i. Easy-to-draw graphic displays.
j. Mouse track ball/touch pad/or writing pad capabilities with *drag-and-click.*
k. Unified consistent *look-and-feel.*
l. PCC terminal security consistent with host system security.
m. Displayed values can be dynamic and refreshed where appropriate.
n. High resolution color printer with menu selection or function buttons.

4.11.3.2 Operators' Interface Requirements

The following are operators' interface requirements:

a. Diagrams should be available to show present and changed database information for process plant and host system monitoring control.
b. Operator should be able to perform multiple tasks.
c. Different types of windows should be available for operator tasks.
d. Operator calls should be available by menu selection of process information and functions.
e. Message and alarm handling should be exactly the same on any display.
f. Operator changes to database values should have confirm and accept steps.
g. Forms-style dialog boxes for multiple database parameter changes should be available.
h. Graphic objects and menu select options to start/stop control and data monitoring applications should be available.
i. On-demand generations and display/printing of previously configured reports should be available.
j. Ability to associate displays to other displays.
k. Flexible trend windows with pop-up selections of trend points and trend parameters should be available.

4.11.3.3 Engineers' Interface Requirements

The following are engineers' interface requirements:

a. Facilities for performing all operator tasks listed above should be available.
b. Ability to reset security to a higher level.
c. Separate display-building window for constructing interface displays.
d. "Fill in the blank" forms for configuration.

4.11.3.4 Others' Interface Requirements

The following interface requirements of others:

a. For non-frequent users, a *user friendly* system is a must. The design of an interface system must include the flexibility to allow users to participate in the development of different interfaces and also the ability to easily make changes.
b. Multiple types of "windows" to all information should be available, as well as multiple ways of accessing the information. One way to access information is to call up the P&ID and select (click) on any instrument, line, or equipment shown. Upon selection, a menu should appear for additional information. An alternative way of accessing information is

COPYRIGHT 2002; American Petroleum Institute

Document provided by IHS Licensee=Sincor Venezuela/5934214100, User=, 08/13/2002 12:13:45 MDT Questions or comments about this message: please call the Document Policy Management Group at 1-800-451-1584.

pattern recognition and key word look-ups, where you either can type in specific plant/equipment information or just use descriptive words.

c. Information inquiries with intuitive selection (key-word, point-and-click and other user friendly ways to access the information).

d. Ability to use common spreadsheet and database programs to analyze data.

4.12 Connection to Other Environments

Connections for applications depend on the data that needs to move between networks, and on the speed and frequency of its movement. The technique used depends on capabilities of the network links, on the limitations on the applications themselves, and on data access authorization. Note the following links:

a. *File links*: In the simplest case, data is transferred between applications on each network via files. File transfer should be used when time is not a critical factor, or where the complexity of linking applications using other methods is not justified. The time factor may be improved by automating file transfer.

b. *Database links*: Data is transferred via shared database tables. This option should be used when time is a more important factor (see 4.10.4).

c. *Application links*: Transferring data directly between applications is required when time is an important factor, and where applications cannot access a shared database. In general, each application should provide a programmatic access that other applications can use. An integration platform should be sought that minimizes the extent of customization required.

Linking computer systems is nontrivial and requires the expertise of an experienced systems integrator.

4.12.1 CONNECTION TO HIGHER-LEVEL COMPUTERS

The plant and corporate networks should be separate to control loading and to provide adequate security. Separation is especially critical if data from the corporate network is used for control purposes on the plant network. Typically, most plant data will move upwards into the corporate network. The connection between the networks needs to be addressed at both the network and application levels.

Connection at the network level depends on the architecture of the networks and on the protocols used. For similar networks, a router should be used in preference to a bridge. This separates the networks and prevents problems on one network from affecting the other. Repeaters should not be used as they do not control traffic between the networks. Dissimilar networks require the use of a proprietary network protocol to minimize interconnection complexity (see 4.6).

4.12.2 CONNECTION TO PEER SYSTEMS

The plant network may consist of a variety of network types as dictated by the peer computer systems used. If a peer computer system, such as a laboratory system, exists on the same plant network type as the PCC, the plant network should be split into separate network segments using a bridge or router. Dissimilar networks require the use of a gateway.

The recommendations described in 4.12 apply equally to the connection of peer computer systems. The only difference may be that time is a more important factor, and data may flow in both directions between the PCC and its peers.

4.12.3 SUBSYSTEM COMMUNICATIONS

Since most process devices will communicate with the DCS, subsystem communication refers mainly to the hardware and software communication link between the DCS and the PCC. It could, in some instances, include other devices or computers that are also required to communicate with the PCC.

The subsystem communications should provide security, data checking, and scheduling:

a. System security should ensure that data transfer between the subsystem and the PCC are authorized. Care should also be taken to ensure that the communications link is secure from physical damage as well.

b. Data checking is a method for checking the data for errors. There are a number of software routines available for checking for false data.

c. Scheduling of data transfers is essential for ensuring that the PCC has the latest information for its programs. Data must be sent from the subsystem to the PCC in the correct time interval.

4.13 Software Reliability

Reliability of the software will in most cases determine the overall reliability of the system. There are two primary principles that should govern how software is structured and implemented to maximize the reliability:

a. Each piece of software is written to minimize failures and to ensure that if a failure is encountered, it will disable that application only.

b. The interaction of multiple applications is built so as not to cause a complete failure of the system.

4.14 Application Programming

Application programming generally falls into two categories: process control/database systems and advanced control technology systems.

First is the process control and database software. These packages normally handle database input and output, user graphical interfaces, database historization, and some advanced control functionality.

COPYRIGHT 2002; American Petroleum Institute

Document provided by IHS Licensee=Sincor Venezuela/5934214100, User=, 08/13/2002 12:13:45 MDT Questions or comments about this message: please call the Document Policy Management Group at 1-800-451-1584.

API RP*554 95 ■ 0732290 0549607 121 ■

The second category includes more complex advanced control software (such as engineering calculations, process modeling, and data reconciliation), unit and plant optimization, and "artificial intelligence" packages, as well as fuzzy logic, neural networks, and expert systems.

4.14.1 CUSTOM VERSUS PACKAGED APPLICATION SOFTWARE

Packaged application software has the advantages of being cheaper and relatively quick to install, generally has better documentation, and is less likely to experience severe commissioning problems. Packaged software is generally configurable. Examples include algorithms for executing control schemes, multivariable control, blend ratio control, and pass balancing. Packaged applications are recommended when they meet the user requirements.

Custom software is coded or programmed to a particular application. Development costs are generally higher and the installation can be significantly longer than that of a packaged software system. Care should be taken to insure that custom software is designed so that it will be easy to operate, maintain, and document. Custom software should be developed using a company-accepted methodology.

4.14.2 APPLICATION ERROR MESSAGE

There are two aspects to the error message issue: operating system messages for the engineer/system manager and process operation messages for the operator.

The operating system messages for the engineer should be comprehensive enough to monitor the PCC system and warn the user when failures have occurred or are about to occur. It is recommended that the messages should be in simple English rather than coded numbers and should be explicit enough that the user can solve most problems without the intervention of the software vendor.

The messages for the operator should likewise be explicit and in simple English. A common problem with application software, especially process control/database systems, is error message overload. It is recommended that methodology to limit and prioritize error messages to the operator be implemented. Important error message must not be lost within a multitude of rather meaningless messages.

4.15 Testing/Development Environment

Where application programs will be developed, testing should be considered carefully. This work may be possible on the PCC system itself. When making additions to an existing in-service system, it is usually desirable to develop and test all software on an off-line developmental PCC system. The development system should be as close as possible functionally to the real system so that database and driver interfaces can be debugged before system commissioning.

4.16 Installation and Support Requirements

This section deals with the recommended practices for the installation and support of computers used for process control.

4.16.1 INSTALLATION

4.16.1.1 Architectural

Control center construction and design considerations are covered in Section 5.

The following items are considerations specific to the installation of process computers in the control center.

4.16.1.1.1 *Traffic planning*: It is recommended that all process computers be placed in a room separate from the control systems and from all operating personnel areas. This separation is recommended for security, power, and operating-condition reasons. Safety considerations may require the computer system to be located away from operating areas.

Adequate floor space should be provided for the existing computer equipment and plans for future expansions. As a minimum, space should be planned according to the computer manufacturer's guidelines. In addition, more room will be required for the computer support items such as documentation storage, work surfaces, and easy access to equipment and facilities.

4.16.1.1.2 *Computer floors*: UL 779 is the recommended standard for safety covering electrically conductive flooring. This standard should be followed to prevent computer equipment damage. The floor should be incombustible.

4.16.1.2 Fire Protection

Provision must be made to protect the equipment from fire and to notify personnel of potentially threatening situations. Installation must include a fire alarm system and a means of suppressing a fire should one occur. Individual states, through their fire marshals, have requirements for fire systems. State and local codes for fire protection systems should be followed.

4.16.1.3 Physical Security

Provision should be made for the physical security of equipment and software. Controlled access is the most normal method of accomplishing this end. One way to ensure physical security is to put computers in a separate room and have access through a locked door. Different levels of security may be desired for CPUs, tapes, and so forth.

4.16.1.4 Electrical Power and Grounding

All power and grounding shall conform to the requirements of the *National Electric Code (NEC)*.

COPYRIGHT 2002; American Petroleum Institute

Document provided by IHS Licensee=Sincor Venezuela/5934214100, User=, 08/13/2002 12:13:45 MDT Questions or comments about this message: please call the Document Policy Management Group at 1-800-451-1584.

API RP*554 95 ■ 0732290 0549608 068 ■

4.16.1.4.1 *Quality of power*: Process computers normally require very clean electrical energy. Care should be taken to insure that the power is free from large voltage and frequency fluctuations.

The FIPS Publication, *Guideline on Electrical Power for ADP Installations*, is a Federal Information Processing Standards publication from the Department of Commerce National Bureau of Standards (Institute for Computer Sciences and Technology). This document discusses hardware grounding, power considerations, and life-safety issues for medium and large automated data-processing centers.

Another standard is NFPA 75 entitled *Standard for the Protection of Electronic Computer/Data Processing Equipment*. This standard recommends that a *secure* disconnect switch (bypassed by a spark gap during maintenance) be used. A Faraday cage should be constructed around the computer room or the building to screen out EMI.

4.16.1.4.2 *Emergency power systems*: Emergency power backup is recommended for the process computer. This decision is based on the applications running on the computer, the reliability of the power source, the maintenance of the data, and the presence of advisory or control programs to help during critical conditions.

If emergency power is deemed necessary, then the latest edition of IEEE Standard 446 should be used. Backup power sources are power conditioners, UPS, emergency generators, or batteries. If a UPS is selected, it is recommended that the UPS system should not service equipment external to the building.

4.16.1.4.3 *Power supply design considerations*: A simple checklist of items to be aware of when sizing power conditioners, UPS, or emergency generators is as follows:

a. Nominal voltage required.
b. Voltage tolerance range.
c. Kilowatts.
d. KVA.
e. Frequency tolerance.
f. Harmonic content.
g. Current inrush.
h. Overload capacity of source.
i. Temperature range of operation.
j. Any special ventilation requirements.
k. Time duration of power backup.
l. Size of air-conditioning load if required during emergency conditions.

4.16.1.4.4 *Noise*: Noise, both electrical and acoustic, generally dictates a UPS and generator room separate from the computer equipment. Noise can be received from the power lines in the form of harmonics, or radiated back out by the battery charger circuits. This means that a standby or reserve power source for a UPS or generator needs to be free of noise and should not have any battery chargers connected to it without proper filtering or conditioning.

4.16.1.5 Heating, Ventilating, and Air-Conditioning

The process computer shall operate without degradation or disruption within the manufacturer's suggested limits.

Control of temperature, humidity, dust, and corrosive contaminants is necessary for the computer room. Temperature monitoring and alarming in the computer room should be available. The computer should be on a separate circuit from the air-conditioning. In addition, there are several special requirements that should be met.

The *NEC*, Article 440, *Air-Conditioning and Refrigeration Equipment*, gives several requirements for refrigeration and air-conditioning installations. ARI 210 offers guidelines. ASHRAE 15 *Standard Safety Code for Mechanical Refrigeration* and ASME codes should also be referenced for refrigeration and air-conditioning installation guidelines.

Sizing: Air-conditioner sizing needs to be based on the expected heat loads during the least favorable time of the year. Consideration should be given to abnormal heat loading due to extra people in the computer room at times of emergency repairs, and so forth.

It is recommended that chemical air purification be installed to remove corrosion-producing gases. This will allow electronics to work much longer without corrosion on the exposed copper, silver, and gold contacts frequently used in computers.

Air-conditioning and air purification equipment should be sized following manufacturer's recommendations.

Air-conditioning backup: Design features which mitigate equipment vulnerability to inadequately conditioned air should be considered. A backup air handler would circulate air upon failure of the primary air handler, thereby eliminating temperature rise at the site of the electronics.

4.16.2 SUPPORT

4.16.2.1 System Software and Data Backups

Monthly image copies are recommended as a base for restoring the system in case of a catastrophic failure. Incremental backups should be performed on a frequency that corresponds to the amount of changes in the database and the importance of the data. As a minimum, weekly incremental backups should be performed to backup any files that changed since the last weekly backup. Restoration is performed using the most current backup.

Additional equipment needs to be provided to allow for on-line backups. This equipment can be as an extra disk, a shadowed set, or a software program to allow writing the data to another computer.

Two copies of the backup should be made. One copy should be stored locally and the other copy should be stored off-site.

COPYRIGHT 2002; American Petroleum Institute

Document provided by IHS Licensee=Sincor Venezuela/5934214100, User=, 08/13/2002 12:13:45 MDT Questions or comments about this message: please call the Document Policy Management Group at 1-800-451-1584.

4.16.2.2 Software Maintenance

Due to the need for continuous operation of a process computer system, maintenance considerations should influence the selection of the computer system. The process computer shall function with limited required maintenance and be designed such that servicing can be performed without system degradation.

The user should obtain the source code for any application software, especially if it is custom coded. Should a vendor company fail some time after the software commissioning or otherwise drop support of a product, the user can then still modify and maintain the purchased software. However, it is not uncommon to encounter proprietary technology in software packages where the vendor will be unwilling to supply source code. In these cases, at least obtain object code from the vendor instead of executable code so that connected nonproprietary software can be upgraded and relinked as the need arises.

This source code language will often be fixed by the selection of the application software packages. If custom software is being written, the user can usually select the source language. Currently, much of the PCC software is written in FORTRAN because of concerns over user support by non-computing personnel. It is recommended that the user consider using a higher level language, such as C or Pascal, because of better code structure and easier subsequent modifications and more powerful built-in functions.

Support for the software in the system will normally come from three different sources. These are (a) from the supplier of the base processor hardware, since the operating system and some support tools are generally supplied with the hardware platform, (b) from the vendors of the various software packages purchased and added to the base platform, and (c) from the end user, since most users will need to maintain the software and applications that they develop.

Support requirements can be discussed in several classes. There is support needed during the normal, on-going business of the plant. This type of support includes routine maintenance and updates, answering questions, and fixing problems that develop.

A common requirement in the "fixing problem" class is 24-hour coverage, sometimes dedicated on-site, or with a maximum 2-hour response time.

"Question answering" should be supported at least 8 hours a day, 5 days per week. Because of the global nature of software use, this is rapidly expanding to 24-hour coverage, 7 days per week.

"Updates" is a longer term situation. Minimum warranty periods should be 1 year. There is also the strong desire to have an enhancement and development for software packages.

Since it is likely that remote maintenance and diagnostic's capability will be required, proper system security procedures should be implemented to insure data and plant control integrity (see 4.9).

4.16.2.3 Documentation

A complete documentation set needs to be established and maintained for the PCC. This set is made up of three parts:

a. Vendor-supplied standard documentation.
b. System integrator-supplied documentation.
c. System user documentation.

A minimum of two sets of documentation is recommended, one set stored locally, the other set stored off-site. At least one set of this documentation should be in electronic format.

4.16.2.3.1 Vendor-Supplied Standard Documentation

System documentation should include the following as a minimum:

a. System operating manuals.
b. System user's guides.
c. System maintenance manuals.
d. Site installation/preparation manuals.
e. System hardware specifications.
f. System software manuals (for example, operating system compilers).
g. Auxiliary software manuals (for example, editors, FORTRAN).
h. Application software manuals.

4.16.2.3.2 *System integrator-supplied documentation*: Documentation supplied by the system integrator should include the following as a minimum:

a. System configuration and cable layout diagram.
b. Cabinet arrangement drawings.
c. Electrical drawings and documentation.
d. Overall system power.
e. Grounding and shielding schemes.
f. Heat loads.
g. All system internal and external connection points and terminations.
h. Complete wiring and cable lists.
i. Complete bill of material and recommended spare parts lists.
j. Source code for application programs, when requested.
k. Initial database and control application documentation.

4.16.2.3.3 *System user documentation*: This section applies to the user's builder and supplied portions of the system:

a. Site specific database.
b. Application programs.
c. Graphic displays and reports.

4.16.2.3.4 *Documentation maintenance*: It is extremely important that all system documentation be up to date with

COPYRIGHT 2002; American Petroleum Institute

Document provided by IHS Licensee=Sincor Venezuela/5934214100, User=, 08/13/2002 12:13:45 MDT Questions or comments about this message: please call the Document Policy Management Group at 1-800-451-1584.

API RP*554 95 ■ 0732290 0549610 716 ■

all changes implemented. Refer to API RP 750 or corresponding OSHA regulations for specifics.

Strong consideration should be given to systems that automatically document any changes made across all databases.

4.16.2.4 Training

Operator, maintenance personnel, and engineer training are an important part of the successful operation of a PCC.

The initial projects at a plant site should extensively train the operators, maintenance personnel, and engineers before, during, and after the installation of a PCC system. Follow-up training for each of the disciplines must be planned on a routine basis to keep proficiency and performance at acceptable levels.

It is recommended that training be performed on the same human interfaces that are used in the plant. Training applications include the dynamic process simulators and the attendant control schemes. It is recommended that the use of additional on-line training help screens also be used, above those help screens for the applications.

SECTION 5—CONTROL CENTERS

5.1 General

5.1.1 SCOPE

This section presents recommended practices for the design and installation of control centers for processing operations. Recommended practices for blast-resistant control centers design is not within the scope of this document.

This document does not cover the application software requirements associated with process control, advanced control, process optimization, and data acquisition.

5.1.2 REFERENCED PUBLICATIONS

The latest edition or revision of the following publications shall, to the extent specified, form a part of this section (see 1.4 for titles and publication details): ANSI Z97.1, API RP 500, RP 540, RP 552, ASHRAE *Handbook* (four volumes), IEEE 484, ISA SP-60, NEC 700-12(a), ISA-S71.04 NEC Article 500, NFPA 70, 493, 496, and OIA Bulletin 631.

5.1.3 GENERAL CONSIDERATIONS

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

As a minimum, the process control operator must be provided with control equipment which will display operating data in a manner to permit unambiguous interpretation of the condition of the process plant operation.

This data will be displayed so that current values, alarm conditions, and historical values are readily available. In addition, the control equipment will provide facilities for the operator to manipulate the operation of the process plant by a combination of controls. These will include manual operation of final control elements, auto/manual switching, controller setpoint adjustment, and the facility to permit emergency shutdown of equipment.

In some cases, the control equipment which interfaces to the process plant input and output signals and which processes the control computations may be located in a separate satellite control building. This document covers both types of buildings.

Some of the factors which should be considered in the design of the layout of these buildings include the following:

a. The type of control equipment to be housed.
b. The number of process units to be controlled and how control is to be integrated.
c. The location of the building.
d. The environment in which the building will be sited.
e. The environment within the control center.
f. Any requirements for future space.
g. Office requirements.
h. Maintenance space and spare parts storage.
i. Facilities for personnel.
j. Personnel and equipment protection.
k. Handicap access.
l. Equipment spacing.

With improvements in data transmission technology and the development of modern communications systems, it is practical to locate control centers remotely from their process plant. This has provided the capability for more than one process plant to be controlled from a control center.

Centralization of control has the following advantages:

a. Improved coordination between different process units.
b. Rationalization of control operator's duties.
c. More effective operations supervision.
c. Reduced installation costs through shared facilities.

Integrated refineries and petrochemical plants can be operated and controlled from a single control center. However, if two or more control centers are used, information flow between centers is recommended.

Industry practice indicates that the highest levels of success in implementing centralized control have been achieved by using electronic transmission and control equipment. While pneumatic transmission and control equipment have been used in central control centers, generally these

COPYRIGHT 2002; American Petroleum Institute

Document provided by IHS Licensee=Sincor Venezuela/5934214100, User=, 08/13/2002 12:13:45 MDT Questions or comments about this message: please call the Document Policy Management Group at 1-800-451-1584.

have been in smaller plants or in installations where transmission distances are short.

Significant improvements have been made in display and control capabilities by the development of microprocessor-based distributed control systems (DCS). These systems have enhanced the benefits of centralized control.

5.2 Control Center Design Considerations

5.2.1 SIZE

Control center size will be determined by the number of process units to be controlled from one location and the amount of auxiliary equipment that center is required to house.

Such equipment may include the following:

a. Terminal racks.
b. Communications systems.
c. Power supplies.
d. Logic cabinets.
e. Auxiliary equipment racks.
f. Air-conditioning.
g. Safety equipment.

In addition, consideration should be given to providing a kitchen and eating area, locker rooms, toilets, showers, conference room, training facilities, process simulators, offices, instrument repair room, and engineering console office. The installation of a process computer normally requires a separate computer room. (See Section 3). The control center should be sufficiently large to accommodate future expansion, including instrument systems requirements, power supplies, and terminations for input and output signals.

5.2.2 SAFETY

5.2.2.1 Area Classification

In classifying areas, the latest edition of API RP 500, as well as other applicable codes, for example, NFPA 497A for chemical facilities, should be used. Generally control centers should be located in "general purpose locations" (as defined in the *National Electric Code*).

Regardless of area classification, it is recommended to maintain the building at a slight positive air pressure to prevent hydrocarbons, corrosive gases, and so forth from entering the control center. Mechanically assisted door openers and closers can improve safety and convenience for pressurized and blast resistant structures. Refer to 5.4.4 for details concerning pressurizing systems.

5.2.2.2 Distances From Process Units

Petroleum refining companies have standards for determing the location of the control center in relation to the operating areas. In general, these requirements are based on the *National Electrical Code* NFPA-70 and API RP 500.

The control center should preferably be located on high ground so that open drainage lines or hydrocarbon spills will not carry hydrocarbon vapors or liquid to the control center. Elevation above the source of hydrocarbon can affect the area classification. At a minimum, the control room should be six to twelve inches above grade or the 100-year flood, whichever is higher. At locations where a prevailing wind is a significant factor, the control center should be located upwind of the process.

5.2.2.3 Protection From External Explosions

It is recommended that new multiunit control center buildings which house instruments, controls, and process computers should be designed to withstand "reasonably expected" refinery-type hydrocarbon explosions to insure the following:

a. Personnel safety from building collapse, fire, and toxic gases.
b. Protection of the control and process computer equipment to allow for the safe and orderly shutdown of the process at the time of the incident.
c. Allowing the control room operator to remain at his post and perform his required duties during the emergency.
d. Preservation of records of events preceding any major occurrence.

In determining the need for blast protection for new control centers, the prime factors considered are the potential risk to operating personnel and the business losses that could result from a damaged control center and consequent inability to operate sections of the plant outside the explosion area.

Minimum requirements for control houses that serve units(s) where no explosion hazard exists include the following:

a. Should meet all local building codes and standards.
b. Should be non-combustible.
c. Should avoid the support of roofs by non-ductile walls.
d. Should not carry out laboratory testing in the control room.
e. Should not have connections inside the building to process sewers or storm sewers.

Furthermore, exterior windows are not recommended. Windows, doors, and glazing materials for interior use should be as follows:

a. Sash and frames for windows should be metal.
b. Doors and frames in walls and interior firestop partitions should be metal.
c. Glass for interior use (doors, windows, and partitions) should be "safety glass" as specified in ANSI Z97.1.

COPYRIGHT 2002; American Petroleum Institute

Document provided by IHS Licensee=Sincor Venezuela/5934214100, User=, 08/13/2002 12:13:45 MDT Questions or comments about this message: please call the Document Policy Management Group at 1-800-451-1584.

API RP*554 95 ■ 0732290 0549612 599 ■

No liquids or gases except steam (maximum 20 psig), instrument air, domestic water, and fresh air should be piped into the control building. If steam is piped to the control room, precautions must be taken to ensure that hazardous substances from the process cannot enter the steam system, and that steam traps and drains are piped to a closed drain system that transports condensate and vapor from the control room.

Battery rooms that are part of a control house building should have direct access to the outside and should not have any direct access to the control room. Hazardous gas detection systems for battery rooms should be considered.

5.3 Control Center Interior Design

5.3.1 GENERAL

The control room is the focal point of the control center and of the refinery. Consideration should be given to providing an area for visitors to be able to view operations without interruption to operators. An observation area separated from the control room by glass paneling has proven effective.

In designing the layout of the control center, the following should be allowed for:

a. A minimum of two entrances should be provided to handle potential emergencies.
b. The layout should be designed so that there are no blind corridors.
c. Entrances should be provided with air locks.
d. Care should be taken to permit the removal of any equipment installed in the control center. Double doors are normally used.
e. Consistent with 5.3.1 item d, corridors should be a minimum of 4 feet wide.

5.3.2 CONTROL ROOM

The control room is the operations area of the control center. The control operator(s) is normally located in this room, together with all necessary operator interface equipment.

The design of this room will be dependent on the type of control equipment employed and whether the equipment is housed in panels, consoles, or a combination of panels and consoles.

5.3.2.1 Control Panels

Because of the construction and size of control panels, it is usual that the control room is designed around the panels. Care must be exercised to ensure that sufficient panel space is provided and that panels are arranged to permit the operator to survey the maximum panel area.

Control panels usually provide a vertical or near vertical surface into which instrumentation is mounted. It is normal to expect a control operator to stand while reading or adjusting panel-mounted instruments. Provision should, therefore, be made for a desk to permit performance of clerical activities.

5.3.2.2 Control Consoles

With the advent of DCS systems, the use of control consoles has gained in prominence. They are particularly suited to the control of process plants from cathode ray tubes (CRT). Consoles usually permit the control operator to carry out his duties while seated.

In addition to the CRTs and their related keyboards, the console may also house alarm annunciators and dedicated instruments to display critical variables, separate switches to initiate emergency shutdown, and communications equipment such as telephones and radios.

Consoles are generally smaller than equivalent control panels and are generally able to be relocated short distances within the control room. It is generally possible to rearrange consoles to account for additional facilities being added to a control room.

Consoles may be the primary source of process information, or they may be used in conjunction with control panels; if so, they should be located a minimum of 6 feet (2 meters) from the panel to permit reasonable access.

5.3.3 AUXILIARY EQUIPMENT AND UTILITIES

Space must be provided for auxiliary control equipment and other control center facilities. The following list covers the most common requirements:

5.3.3.1 Auxiliary equipment racks should be located in a separate equipment room or directly behind the associated control panel section.

5.3.3.2 Termination cabinets should be located adjacent to the field cable entry point into the control building. They would normally be in the same room as the auxiliary equipment racks.

It is common practice to terminate field wiring on marshaling panels in the equipment rack room. The completion of instrument loops is achieved by making innerconnections between these marshaling panels and the equipment terminals. This arrangement has these advantages:

5.3.3.2.1 Not having to make inconvenient changes to field wiring.

5.3.3.2.2 Being able to make subsequent configuration changes or additions and deletions to instrument wiring without the need to enter secure equipment housings.

5.3.3.2.3 The ability to unscramble wiring.

5.3.3.3 Computers normally are located in a separate computer room. This room should also house computer peripherals such as mass storage devices, system terminals, and system logging printers. (See Section 3).

COPYRIGHT 2002; American Petroleum Institute

Document provided by IHS Licensee=Sincor Venezuela/5934214100, User=, 08/13/2002 12:13:45 MDT Questions or comments about this message: please call the Document Policy Management Group at 1-800-451-1584.

5.3.3.4 A separate utilities room should be provided to house the uninterruptible power supplies (UPS) and other power supplies required for the control systems, computers and auxiliary equipment, HVAC, lighting, and emergency lighting circuits.

Batteries required for the UPS should be located in a dedicated battery room. This room should be vented to the outside of the control building to readily permit the egress of hydrogen formed in the batteries. A doorway should also be provided to the outside of the building from this room. The interior surfaces of the room should be acid spill proof, and acid-proof racks should be used. Refer to NFPA 70 and IEEE 484 for additional information.

A separate building is usually required for motor control centers and large power handling systems not associated with the control center.

5.3.3.5 Consideration should be given during the building design phase to the routing of wiring and/or tubing among the auxiliary equipment, control consoles, and field termination areas. Lack of planning in this area could result in last minute trenches or overhead cable trays being installed, thereby resulting in congestion and poor appearance.

Consideration should be given to installing a computer-type raised floor to provide additional flexibility, both in the control room itself and for computer or other electronic systems rooms. Refer to 5.3.6 for details of floor design.

5.3.3.6 Office space for operations supervision is often included within the control center. The extent to which offices are provided is subject to the operational organization structure and job functions. Space allocation differs from plant to plant and is usually dictated by company policy. Such factors can vary from time to time, and the design of the building should permit subsequent changes in layout.

5.3.3.7 A mechanical equipment room should be provided to house air handling equipment, including air-conditioning, filtration, and purifying equipment. Air-conditioning equipment should not be mounted on the roof of the control building because of problems of maintenance access and, particularly in the case of blast-resistant buildings, because of lack of protection. Raised floors are not recommended for mechanical equipment and rooms.

5.3.3.8 Amenities to be provided within the control center include the following:

a. Sanitary facilities in accordance with local, state, and federal codes.

b. Lockers and change rooms.

c. Kitchen facilities.

d. Drinking-water fountains.

e. A storage area for miscellaneous supplies.

f. A janitorial supply closet.

g. A protective equipment room.

h. Operator training facilities.

i. Handicap access.

5.3.3.9 A *light repair* instrument maintenance facility including an area for specialized test equipment may be provided when space and organization allow.

5.3.3.10 A generous space allowance for future needs is recommended, particularly when a blast-resistant design is used.

5.3.3.11 If it is considered necessary to locate a laboratory in the control center building, there should be no direct access between the laboratory and the control center. The laboratory should be separated from the rest of the control center by a permanent partition and be provided with its own air-conditioning system, vent hoods, and safety exhaust systems.

5.3.3.12 Fresh breathing connections or other air breathing devices should be provided as required.

5.3.4 LIGHTING

Lighting has a significant impact on the efficiency, comfort, and general effectiveness of the control room operator. With the proliferation of lighting fittings, fixtures, types of illumination, and influences of floor and wall colors and textures on the effectiveness of lighting, it is recommended that qualified personnel be used to perform the lighting design.

CRT-based operator interfaces require special lighting provisions. Lighting fixtures should be arranged and the surrounding environment selected to ensure that glare is eliminated. Because CRTs emit light, the level of lighting in the area of CRTs is subject to the preference of individual operators. Some prefer a relatively high-intensity of background light at their workstation, while other are more comfortable in dimmer surroundings. Provision should be made to permit the background lighting and the individual operator working space lighting to be independently adjustable.

Current practice calls for the following typical minimum lighting intensities in various areas of the control center (see table 4).

Factors establishing the general lighting intensity away from panels or consoles are contingent upon the nature of the other duties performed by the control room operators. The use of devices to minimize glare is recommended.

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

An emergency lighting system is required. The system should be connected to an emergency supply so that in the

COPYRIGHT 2002; American Petroleum Institute

Document provided by IHS Licensee=Sincor Venezuela/5934214100, User=, 08/13/2002 12:13:45 MDT Questions or comments about this message: please call the Document Policy Management Group at 1-800-451-1584.

API RP*554 95 ■ 0732290 0549614 361 ■

Table 4—In-Service Lighting Requirements

Area	In-Service Intensity (Lumens/Sq.Ft.)	Elevation
Vertical control panels	50	All operator interface areas
Consoles	30	All operator interface areas
General control room areas	30	Floor
Back of panel areas and auxiliary equipment rooms	50–80	Floor

Note: /sq.ft. = per square feet. Local task lighting may be required at greater illumination levels.

event of a power failure, orderly limited operation or shutdown can be executed. In addition, some or all of the lighting in the general control room area should be connected to the emergency system. In all cases, local electrical codes should be followed.

In non-operating areas, only strategic locations such as the lighting control panel and exit doors require connection to the emergency lighting system.

5.3.5 CEILING

The minimum recommended floor-to-ceiling height is 10 feet (3 meters) to accommodate equipment and provide a good appearance. A nondusting type of acoustic tile or board with an exposed grid suspension system forms an economical ceiling. There should be sufficient space between the ceiling and the roof framing members to allow for trays, ducts, and lighting fixtures.

5.3.6 FLOOR DESIGN

An access or computer-type floor is often used in rooms with electronic instrumentation. This type of floor simplifies the routing of cables between control panels and auxiliary equipment or consoles. The use of underfloor cable trays may be considered for organized routing. Additions or revisions to the control room equipment are also simplified. Care should be taken, however, with the laying of cables in the underfloor space below computer flooring to ensure that individual cables are not locked in place by overlaid cables. A floor height of 18–24 inches (0.5–0.6 meters) from the concrete subfloor to the top of the floor is recommended.

The floor must be designed to hold the full weight of control panels and other equipment without deforming or sagging. Should it be required to install particularly heavy equipment, or if the equipment is likely to vibrate, a support structure isolated from the computer flooring should be used. When control panels are used, a perimeter trench around the control room is sometimes used. The trench should be 12–18 inches (0.3–0.5 meters) deep and should extend from beneath the control panel out to the control room walls. A series of interconnecting trenches should lead from operator consoles and desk-type equipment to the perimeter trench. Computer-type floor or other easily removable material should cover the trenches and rear panel areas.

An alternative to the computer-type floor is a cable spreading and distribution room below the control room. This design provides a place for installation of auxiliary equipment; however, blast-resistant construction costs increase significantly for multistory buildings.

The floor covering of the control room should be vinyl material, plastic laminated, or carpet with electrical grounding properties. Nonoperating areas should be vinyl, ceramic, or quarry tile. Refer to 5.3.8 for static electricity design requirements.

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

5.3.7 PAINTING

Color can be used to create an atmosphere of comfort and well-being.

Interior and exterior painting should follow the industrial standards in force. Care should be taken to produce an easy-on-the-eye color scheme which harmonizes with the equipment color scheme. Good design calls for flat or semigloss surfaces of low-contrast colors. A smooth color graduation from floor to ceiling and color continuity throughout the building should be considered.

Control panels and consoles should be painted in subdued tones so as not to draw attention away from instruments and CRTs.

5.3.8 STATIC ELECTRICITY

Static electricity can adversely affect system operation causing damage to electronic components. Any flooring material must be of a type that minimizes the effects of static electricity. Chair coverings should be made of materials that resist the generation of static charge.

In general, both furniture and flooring must be designed for computer room installations. Proper humidity control in the area will also reduce the incidence of static discharges.

5.4 Internal Environment

5.4.1 GENERAL

This section presents the common practices and considerations for the design and selection of environmental equipment used to maintain conditions that are the following:

COPYRIGHT 2002; American Petroleum Institute

Document provided by IHS Licensee=Sincor Venezuela/5934214100, User=, 08/13/2002 12:13:45 MDT Questions or comments about this message: please call the Document Policy Management Group at 1-800-451-1584.

API RP*554 95 ■ 0732290 0549615 2T8 ■

a. Conducive to human comfort.
b. Required to protect the instrumentation located in control centers.

To perform these functions, heating, ventilating, and air-conditioning equipment (called HVAC systems) must be installed. HVAC is the process of treating air to provide ventilation and to control its temperature, humidity, cleanliness, and distribution.

5.4.2 HEATING, VENTILATING, AND AIR-CONDITIONING

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

a. Inside design conditions.
b. Outside design conditions.
c. Size and physical characteristics of the control center.
d. Average number of occupants and degree of activity anticipated.
e. Heat load from the equipment housed in the control center, including provisions for future expansion.
f. Quantity of air assumed for ventilation and leakage through doors, windows, and wall penetrations.
g. Manufacturer's site planning guides for the installed equipment.
h. Positive pressure design.

The HVAC system should be based on both winter and summer outside/inside design conditions and should consider both space heating and cooling requirements.

Most modern control centers are equipped with a central system that provides heating, cooling, filtering, and humidifying/dehumidifying of the atmosphere, as well as a positive pressure to prevent the ingress of flammable and corrosive gases and vapors.

The ventilation equipment must operate continuously to circulate the conditioned air (a mixture of both recirculated and fresh air) through registers or diffusers in the ceiling or floor of the control center. The proportion of recirculated to fresh air is usually set by manually positioning dampers in the ductwork.

Thermostatically controlled elements located in the air system are required to heat/cool the incoming air depending upon ambient conditions. If the outside air temperature is likely to fall to less than 15°F (–10°C), a preheat element can be added to heat the incoming fresh air. Geographic location and climatic conditions at the control center and the instrumentation housed determine air-conditioning load and humidity control requirements.

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

Piping containing air-conditioning refrigerant or other liquids or vapors should not be run in the control room or equipment rooms housing electronic equipment.

Each unit of the air-conditioning system should be equipped with air filters capable of removing in excess of 90 percent of particulates with a maximum particulate size of 0.01 micron permitted. Refer to the ASHRAE *Handbook.*

An acid gas removal system should be included as a part of the air-conditioning system to reduce levels of hydrogen sulfide and sulfur dioxide to 3 parts per billion (ppb).

The air-conditioning units should meet the area electrical classification.

The air-conditioner control system should be designed to automatically activate the redundant unit, if supplied, upon failure of the primary unit. The control system should permit selection of either unit as primary or standby.

5.4.3 AIR PURIFICATION

In addition to providing for human comfort, air purification is necessary to protect the instrumentation in the control center against corrosion, abrasive particles, conductive particles, and potentially hazardous fire or explosion conditions. Air purification includes the following:

a. Filtering suspended particles using either fiber or electrostatic-type filters.
b. Eliminating hydrocarbon vapors or gases by locating the air inlet duct per Section 5.4.5.
c. Removing corrosive vapors (such as hydrogen sulfide, sulfur dioxide, and ammonia) by providing a filter system with an absorption media. (Refer to the ASHRAE *Handbook* or filter manufacturer's literature for information on the selection of the equipment and filter media required for specific applications.) Manufacturer's site planning requirements and recommendations should be consulted.

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

5.4.4 POSITIVE AIR PRESSURE SYSTEMS

Control centers should be designed to prevent the entry of flammable and corrosive atmospheric vapors or gases. This is usually accomplished with a positive pressure ventilation system using a clean air source (see 5.4.5) in conjunction with effective safeguards against ventilation failure. In case of an external fire or spill of hazardous material, the air-conditioning system should be switched to total recirculation with no intake of outside air.

There are two requirements for a positive pressure ventilation system in accordance with NFPA 496, Chapter 3:

COPYRIGHT 2002; American Petroleum Institute

Document provided by IHS Licensee=Sincor Venezuela/5934214100, User=, 08/13/2002 12:13:45 MDT Questions or comments about this message: please call the Document Policy Management Group at 1-800-451-1584.

a. The system should be capable of maintaining a pressure of at least 0.1 inch of water (25 Pa) in the control center with all openings closed.
b. The system should be capable of providing a minimum outward air velocity of 60 feet per minute (20 meters per minute) through all openings, including all doors and windows and any other openings capable of being opened.

In addition, the system should be capable of providing a minimum of six air changes per hour when air-conditioning is not provided.

Air-conditioning can reduce this requirement to 10 to 20 cubic feet (0.3 to 0.6 cubic meters) of fresh air per minute for each occupant.

Air pressurizing (ventilating) equipment should be mounted inside the control center for blast-resistant building designs.

Ventilation should be by motor-driven backward-bladed centrifugal fans. Failure of the positive air pressure system should actuate both a visual and audible alarm. Provisions must be made to energize the air pressurizing system safely after an interruption. Minimum precautions include the following:

a. Using a flammable vapor detector to determine when it is safe to energize the controls.
b. Providing a fan motor, disconnect switch, and associated wiring system that comply with the area classification in force when the positive air pressure system is not operating.
c. Providing electrical control circuitry to ensure that the fan is in operation prior to energizing any other circuits.
d. Providing electrical control circuitry to ensure that, in Division 1 areas, all HVAC circuits must be disconnected on failure of the air pressurizing system and remain disconnected until such circuits are manually reset.

5.4.5 FRESH AIR INTAKE

The source of air for positive air pressure systems in control centers should be free of flammable vapors, gases, corrosive contaminants, and other foreign matter.

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

When a control center is located in the midst of a process area, ducting may be required. Ducting must be constructed of a noncombustible material, free of leaks, mechanically protected, and corrosion resistant to prevent the admission of hazardous vapors to the control center via the fan suction line.

5.4.6 NOISE

Noise within the control center, especially within the control room, should be minimized to do the following:

a. Reduce the possibility of hearing damage and physical discomfort.
b. Enable effective speech communication either directly or by telephone, radio, intercom, and so forth.

For these reasons, air-conditioning equipment should not be located within the control room. Even if it is located in a separate room of the control center, consideration should be given to noise levels generated by both equipment and the flow of air. Soundproofing materials, vibration mounts, and flexible connections to duct work may have to be used.

Other noise-producing devices (such as power supplies, typewriters, and printers) may have to be located outside of the control room to limit the noise in the operating area. The addition of sound absorption materials should be considered to reduce the noise level [typically maximum of 55 dB(A)].

5.4.7 HAZARDOUS VAPOR

Hazardous vapor includes flammable and corrosive vapors and gases. Hazardous vapor detection and alarm systems should be installed in control centers where there is any possibility of the entry of such vapors.

In particular, flammable gas detectors should be installed in buildings which have reduced the electrical area classification by the installation of a positive air pressurization system.

Hydrogen sulfide and flammable gas detectors should be installed in the fresh air intake ducting. They should generate an alarm when concentrations rise above normally expected levels and automatically close inlet air flow to the building.

Chemical filters on make-up air are recommended to protect personnel and equipment for control centers located in plant areas where corrosive vapors and gases are present.

5.4.8 FIRE PROTECTION

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

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

a. A system of ionization and optical smoke detectors with audible and visual alarms.
b. Portable extinguishers suitable for indoor electrical fire service.

The location of underfloor detectors should be marked on floor tiles for ease of location, particularly for testing. Other rooms and corridors should be provided with water extinguishers and extinguishers for electrical fires as appropriate.

A manual (protected actuation) fire-warning system should be installed.

COPYRIGHT 2002; American Petroleum Institute

Document provided by IHS Licensee=Sincor Venezuela/5934214100, User=, 08/13/2002 12:13:45 MDT Questions or comments about this message: please call the Document Policy Management Group at 1-800-451-1584.

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

a. Sound alarms throughout the protected area.
b. Shut down the air-conditioning and close fire dampers.
c. Activate an audible alarm in the control panel until the fire condition is fully actioned.
d. Report on any fault in the detection system and provide audible and visual warnings indicating the affected zone.
e. Provide warning in the event of mains or battery failure.
f. Alert the fire brigade by a direct link system, manual or automatic.

Emergency exits and escape routes should be clearly indicated.

5.4.9 ELECTRICAL GROUNDING

Reliable ground systems should be provided to electrically ground panel boards, computers, consoles, and related control equipment. Consult manufacturer's recommendations for equipment grounding requirements. For additional information on electrical grounding, see NFPA-70, Article 250, API RP 552, and API RP 540.

5.4.10 ELECTROMAGNETIC INTERFERENCE

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

To assist in reducing radio frequency interference, the walls of computer rooms and other rooms containing electronic equipment should be of aluminum-faced fiberboard or other suitable materials. These walls should extend from the subfloor into the ceiling space. Confining radio communication in the control building to properly grounded base stations will eliminate problems from this source. If handheld radios are used, their antennas should be no closer than 3 feet from electrical equipment and cables.

Warning signs should be placed on entrances to rooms housing sensitive equipment.

For additional information on electromagnetic interference, see API RP 552.

5.5 Satellite Instrument Houses

5.5.1 GENERAL

The development of DCS systems and split-architecture electronic instrument systems provides the opportunity to mount the processor portion of the system in a location remote from the display portion. The choice exists to locate the processor portion in a rack room in the control center or to provide a separate satellite instrument house adjacent to the process plant.

Outside operator workstations are sometimes located in satellite instrument houses; however, it is recommended that the room housing electronic equipment should be unmanned, and the workstation should be located in a separate room.

Satellite instrument houses may be used to house equipment dedicated to one process unit or shared by a number of units.

5.5.2 LOCATION

Satellite instrument houses should, wherever possible, be installed in unclassified locations in accordance with article 500 of the NFPA and API RP 500. The building should be designed to blast-resistant standards if either of the following conditions exists:

a. A satellite instrument house is used to accommodate equipment shared by two or more process units and is in a location where it could be damaged by an explosion in the refinery.
b. The satellite house is dedicated to a single process unit but could be damaged by an explosion from some other source. Otherwise, non-blast-resistant construction may be considered.

5.5.3 CONSTRUCTION

The satellite house construction is dependent on local requirements and site standards. It may be a custom-built building mounted on a concrete slab using reinforced concrete and masonary, steel framed with metal sheeting, of self-supporting wafer construction with steel or glass reinforced plastic coatings or other suitable materials. Or, the satellite house may be a prefabricated self-contained, transportable building. The roof should be designed to withstand anticipated weather loads and constructed to prevent damage resulting from construction, installation, and maintenance activities. The roof pitch should be a minimum of 4 percent. All metal surfaces should be thoroughly cleaned and free from rust and scale and painted in accordance with site painting standards. All concrete and concrete block surfaces should be thoroughly cleaned and sealed to prevent the formation of concrete dust and prevent moisture intrusion.

5.5.4 HVAC SYSTEM

Each satellite house should be provided with air-conditioning, chemical filtration, humidity control, and heating units for the control of temperature and cleanliness of air (see 5.4.2).

The system should be designed to maintain conditions suitable for the equipment in the satellite house. The cooling

COPYRIGHT 2002; American Petroleum Institute

Document provided by IHS Licensee=Sincor Venezuela/5934214100, User=, 08/13/2002 12:13:45 MDT Questions or comments about this message: please call the Document Policy Management Group at 1-800-451-1584.

API RP*554 95 ■ 0732290 0549618 T07 ■

and heating capacity of the system should be sufficient to handle all equipment in the house plus an allowance for future expansion. The need for backup HVAC equipment, louvers, or vents should be considered.

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

5.5.5 AUXILIARY EQUIPMENT

Satellite houses should be equipped with the following:

a. A smoke detector system.
b. Portable fire extinguishers or a fire-extinguishing system suitable for electrical fires, and automatically activated by the smoke detector system.
c. Emergency lights—Battery backup emergency lights should be supplied, a minimum of one unit at each end of the house. Battery operation time should be a minimum of 1-1/2 hours [per NEC 700-12(a)]. Emergency lights should have a power failure relay that causes them to turn on when AC power is lost.

5.5.6 POWER DISTRIBUTION AND WIRING

All power, signal, and alarm wiring should be provided in accordance with the *National Electrical Code* and other applicable codes.

The power distribution system should include one or more UPS systems to power the control system and signal transmission loops. Dual power feeders should be considered. Power wiring should be designed using plenum-rated cable and segregated from low-voltage cables and equipment where possible in accordance with API 540.

Should wiring be routed below floor level, care should be taken to ensure that moisture is unable to collect.

5.5.7 LIGHTING

Lighting should provide illumination levels between 50 and 80 lumens/sq. ft. at floor level within the house.

Exterior light fixtures should be provided at each exterior door. These fixtures should be equipped with at least the equivalent 100-watt incandescent lamps and should be controlled by a photoelectric device with a bypass switch.

5.5.8 INTERNAL LAYOUT

The internal layout of the building should be as efficient as possible. Equipment should be mounted in cabinets and located to provide maximum access to both sides of the equipment.

5.6 Control Consoles and Panels

5.6.1 GENERAL

The purpose of control consoles and panels is to aid operating personnel in maintaining efficient and safe performance of the process plant for which they are responsible from a location remote from the plant.

The instrumentation mounted in the console or panel must provide current and historical plant operating data as well as warn of plant malfunctions.

5.6.2 CONSOLE STYLES

The operator interface for DCS and computer systems is mainly via CRT and keyboard combinations. These are usually mounted in freestanding consoles.

The CRTs may be mounted singly or in piggyback style in the vertical face of the console. It is also common for operators to access data via touch-sensitive screen or by use of a trackball or mouse.

General industry practice dictates that a minimum of two operational CRT displays, together with their dedicated keyboards, are necessary to provide sufficient data and access to controls for safe plant operation. It is recommended that at least one additional CRT/keyboard set be provided to allow for malfunction of one of the other sets.

DCS/computer consoles are also likely to house auxiliary equipment such as system loading devices, indicators, recorders, alarm annunciators, and various push buttons and switches to display and/or control critical plant variables. Hard copy printers and screen copiers are also sometimes provided.

Console configurations may be multiunit, in-line or wraparound styles. Heights vary, but most are designed for operation from a seated position. A writing surface is recommended.

It is most common that DCS consoles be provided as standard equipment by the DCS vendor. Usually the vendor will provide for some degree of customization of the standard design to meet user's specific requirements.

Other types of consoles are those dedicated to a specific function especially when used in conjunction with control panels. These include (among others) compressor surge control systems, compressor/pump vibration detector systems, and so forth.

A typical console is shown in Figure 13.

5.6.3 SPACE CONSIDERATIONS

Clearances of 4 feet (1.2 meters) should be provided around consoles to permit adequate operations and maintenance access. Console doors should be removable to accommodate hardware servicing and ready access to all wiring.

5.6.4 DCS/CRT INSTALLATION CONSIDERATIONS

Many signals in video display consoles are high frequency, low-level signals making them susceptible to noise from power, ground, or adjacent signal wires. Consequently, signal protection should be provided by means of

COPYRIGHT 2002; American Petroleum Institute

Document provided by IHS Licensee=Sincor Venezuela/5934214100, User=, 08/13/2002 12:13:45 MDT Questions or comments about this message: please call the Document Policy Management Group at 1-800-451-1584.

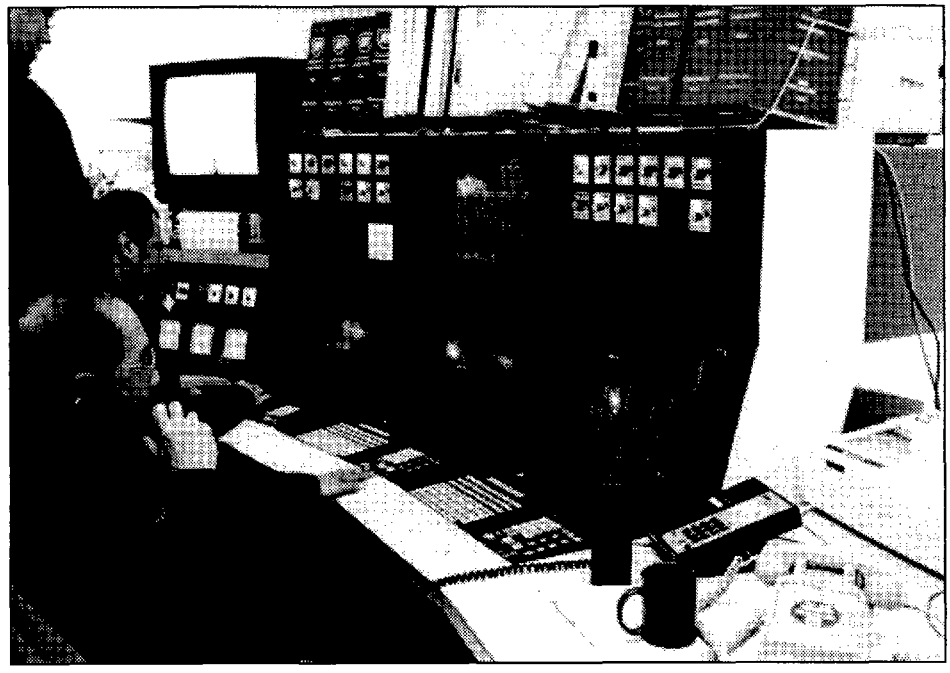


Figure 13—Typical Console

shielded cable. Individual signal wires must be of twisted pair construction. Ground leads should be kept as short and as straight as possible with few connections. Some video display console installations require dedicated system earth grounds. Signal cables should not be routed along the same cable ways as power cables nor routed close to electric motors or other equipment capable of generating significant amounts of electromagnetic interference. Cable length should be kept to a minimum to avoid excessive cable capacitance and impedance, which may lead to signal attenuation and distortion. Long cable length also increases the possibility of electrical noise pickup.

Radio frequency interference may impact the normal operation of console equipment; therefore, sources of radiation such as portable radio transmitters should be operated away from consoles and other control center equipment. However, the use of remote transmitters with carefully placed and shielded console handsets will permit console operators to communicate with the field and will not have an adverse effect on console equipment.

Site-planning considerations are detailed in vendor preinstallation planning guides. These guides are available from vendors and should be used as references during the engineering of the control center.

5.6.5 PANEL STYLES

5.6.5.1 General

The type of panel selected is dependent on a number of factors such as space available, need for graphic displays, number of instruments per operator, and so forth. Since many users have different concerns in panel design, the following typical designs are presented for consideration rather than as recommendations.

Panels may be freestanding cubicles or be built into the control room and extend from floor to ceiling.

Analog displays are usually mounted in the vertical or near vertical face of the panel with alarm annunciators generally mounted above. It is common for the alarm annunciators to be tilted forward of the vertical plane for better visual access.

5.6.5.2 Conventional Panels

A conventional panel is defined as a panel with instruments, mounted in horizontal and vertical rows.

5.6.5.3 Semigraphic Panels

The semigraphic panel combines the compactness of a conventional panel with a process flow plan located above grouped instruments. Semigraphic panel board shapes are shown in Figure 14.

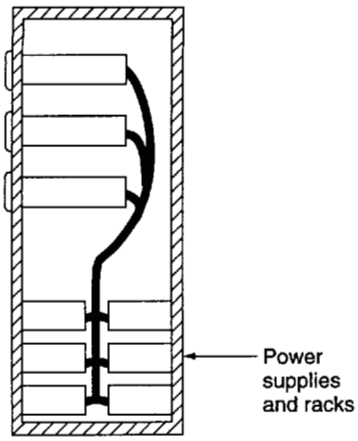
5.6.6 INSTRUMENT ARRANGEMENTS

Instruments should be arranged in configurations that reflect the process flow.

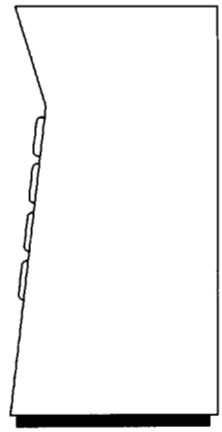
A system that enables an operator to quickly identify any particular instrument is desirable and should be considered in the panel layout.

COPYRIGHT 2002; American Petroleum Institute

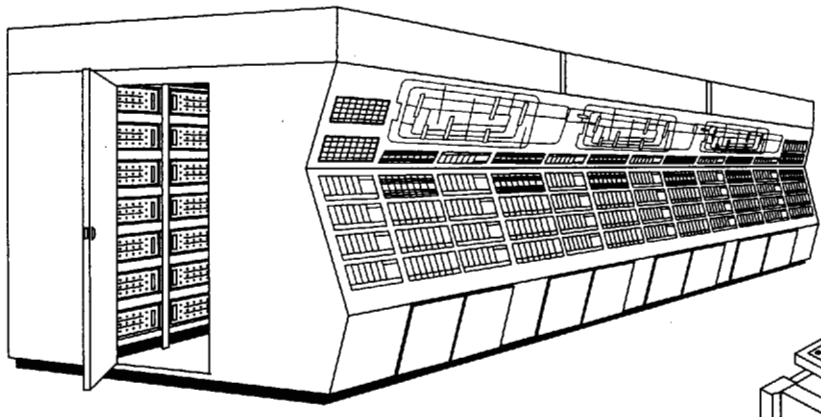
Document provided by IHS Licensee=Sincor Venezuela/5934214100, User=, 08/13/2002 12:13:45 MDT Questions or comments about this message: please call the Document Policy Management Group at 1-800-451-1584.



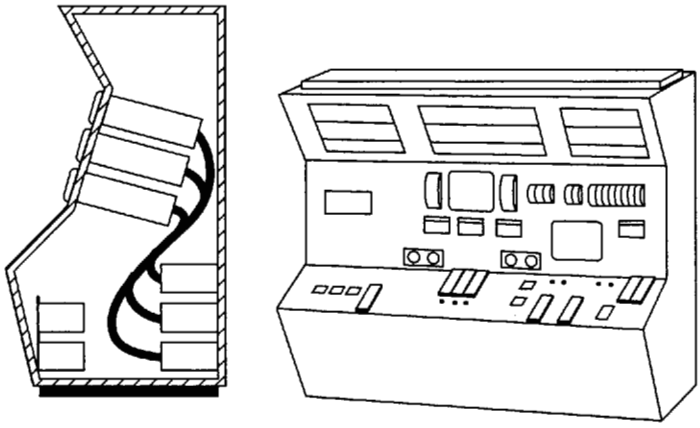
A. VERTICAL FLAT-FACED PANEL



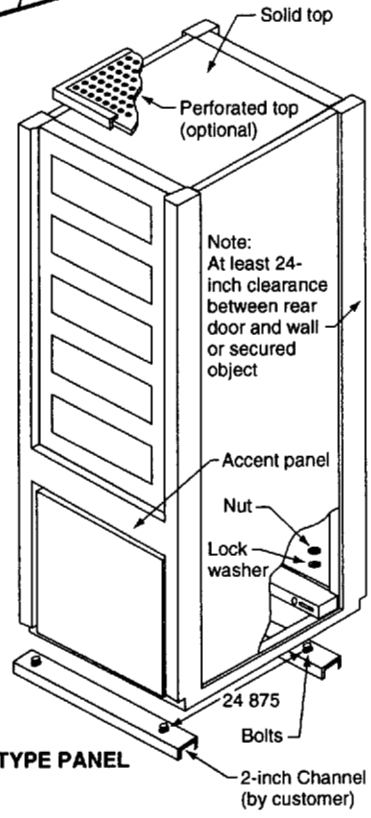
B. VERTICAL PANEL WITH INCLINED SECTIONS



C. WALK-IN PANEL



D. SLOPING FRONT-TYPE PANELS



E. CABINET-TYPE PANEL

Figure 14—Typical Panel Shapes

COPYRIGHT 2002; American Petroleum Institute

Document provided by IHS Licensee=Sincor Venezuela/5934214100, User=, 08/13/2002 12:13:45 MDT Questions or comments about this message: please call the Document Policy Management Group at 1-800-451-1584.

Nameplates, color codes, or symbols frequently are used. Spare panel space, about 20 percent, is recommended to allow for future modification and expansion.

Normally, a limitation is placed on the maximum and minimum heights for mounting instruments on the panel. Typical vertical density is three or four rows.

The density of instrument varies with the type of panel, type of instruments, complexity of the process, and preference of the user (see also ISA SP-60).

5.6.7 SPACE CONSIDERATIONS

Clearance between the back of the panel and auxiliary equipment racks, located along the wall, should be a minimum of 4 feet (1.2 meters).

5.6.8 FABRICATION

5.6.8.1 Control Room Panels

Control room panels are usually freestanding in the form of a box, with a panel front bolted or welded to the frame.

Louvered openings and cooling fans should be provided to remove heat. Heat-producing items should be mounted in the higher portions of the panel to prevent heat from coming in contact with other equipment in the panels.

Cables, conduit, pneumatic tubing, or piping entering or leaving the panel should be provided for in the panel-supporting structure through the use of bulkheads or conveniently located termination points. Consideration should be given to the most convenient point for power and signals to enter the panel.

5.6.8.2 Field Panels

Field-mounted panels are usually made of standard steel or corrosion resistant thermoplate. They may be located in areas where atmospheric corrosion is severe. Field panels may be enclosed and should have rear-access doors for service. Doors should be gasketed and furnished with latches (preferably 3-point locking). Air purging may be required for environmental reasons as well as for electrical safety. The panel should be provided with a steel top and canopy with lighting installed beneath the extended canopy. The framework should be made of structural steel shapes. Lifting lugs should be provided for field handling. Instrument heat dissipation must be provided. Figure 15 illustrates typical field panels.

Special consideration should be given to environmental and local conditions in the selection of finishes for outdoor mounted panels and material.

5.6.8.3 Auxiliary Racks

Racks may be used to house control system components. Racks should be freestanding and framed in structural steel shapes. Environmental conditions may require that they be enclosed and provided with doors.

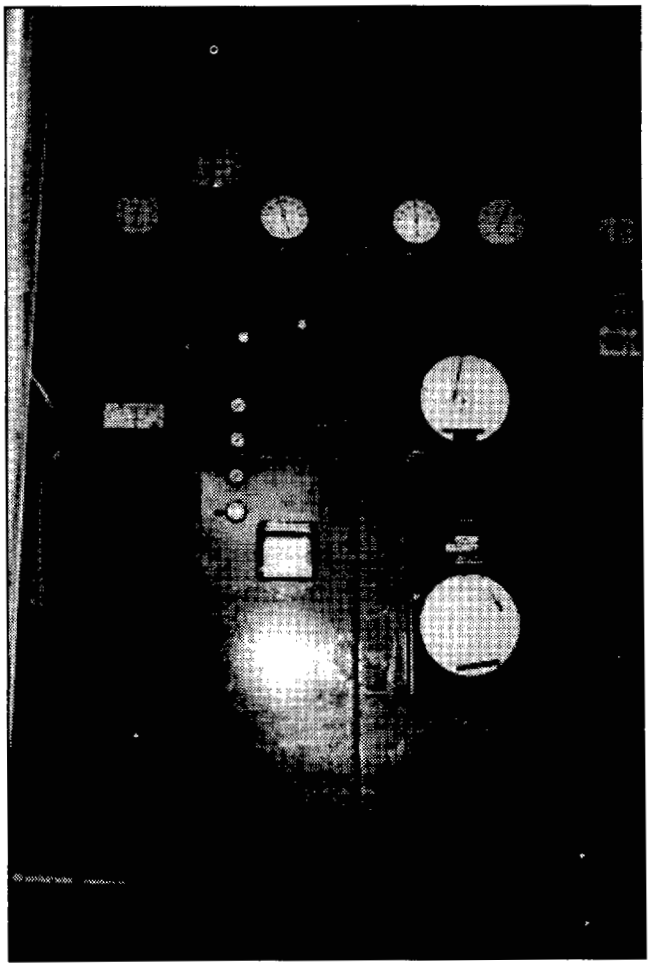


Figure 15—Typical Field Panels

5.6.9 ELECTRICAL CONSIDERATIONS

5.6.9.1 Electrical Installation

Refer to API RP 540 for detailed information concerning electrical installation. Electrical installation should be in accordance with the latest edition of the *National Electrical Code*, local codes, and users' special plant requirements. The area classification and instrument components will determine the minimum enclosure, conduit, and sealing requirements. Wiring laid in forced- or return-air plenums or ducts in ceilings or floors must be plenum-rated and non-toxic when exposed to fire.

It is important to review the instrument supplier's engineering data covering grounding, shielding, shield grounding, fusing, wiring separation, and accessibility of components for removal and maintenance. For ease of maintenance and checking, it is sometimes desirable to terminate incoming and outgoing field leads in auxiliary racks and to mount in the racks such items as power supplies, current alarm relays, annunciator components, loop protection auxil-

COPYRIGHT 2002; American Petroleum Institute

Document provided by IHS Licensee=Sincor Venezuela/5934214100, User=, 08/13/2002 12:13:45 MDT Questions or comments about this message: please call the Document Policy Management Group at 1-800-451-1584.

API RP*554 95 ■ 0732290 0549622 438 ■

iary devices for analyzers, and resistors for electronic instrument inputs (see API RP 552).

All incoming and outgoing electrical leads should be terminated on suitably enclosed terminal strips. AC wiring should terminate on separate strips from DC wiring (refer to 5.6.9.4). Special consideration must be given to the requirements of intrinsically safe installation.

AC wiring must be run in separate conduits or ducts from DC wiring; AC signal wiring (for relays, and so forth) can be carried in twisted and shielded packs. If inductance problems are anticipated, the conduits, trays, or ducts should be separated as far as practical to avoid signal distortion.

DC signal wiring should be sized to carry the anticipated load; however, it should generally not be less than 20 AWG stranded for reasons of mechanical strength.

Thermocouple extension wire should be color coded to ANSI standard. Each wire end for all signal wiring should be tagged for identification by means of a printed slip-on sleeve, self-stick label, or similar permanent marking.

Termination strips should be provided at all shipping section joints for interpanel section wiring. Terminals should be on both sides of the joints with short interconnecting jumper leads provided between the terminals. Terminals should be enclosed in boxes, and wires should be pulled back in panel boxes for shipment. Plug and socket-type connections may be used instead of terminals to simplify field installation and permit factory checkout of interwiring between panel sections or between panels and auxiliary equipment racks.

5.6.9.2 Electrical Supply

AC power supply to the panel is usually single phase 120-volt, 60 hertz. DC-power supply required for loop power to electronic instruments may be furnished from externally mounted common power sources, back-of-panel mounted instrument power units, or power supplies built into the receiving instruments.

Refer to the NFPA 70 and API RP 540 for additional information.

Power wiring should be sized for the anticipated electrical load with allowance for future expansion.

The NFPA 70, local codes, and plant practices must be considered in determining the acceptable color coding for AC power wiring.

Each device requiring AC power should be wired so that when wires are removed from any one device the following conditions will be met:

a. Power will not be disrupted to any other device.
b. Ground will not be broken from any other device.

Twenty percent spare space should be provided for power wiring. It is recommended that each panel section have 120-volt power outlets installed. These outlets should be powered independently of instrument power supplies and are used to power portable tools or test instruments. Generally, the source of supply for such outlets is normal plant power rather than emergency or UPS power.

5.6.9.3 Disconnect Switches

Separate disconnect switches for each cabinet are recommended. Each disconnect switch should be clearly labeled to identify the particular instruments or alarm unit served by that switch. Each 120-volt, AC-powered electronic instrument should be provided with a separate power disconnect. A standard 3-pin grounding or twist-lock plug may be used instead of a switch if permitted by local electrical codes.

5.6.9.4 Terminal Blocks

All wiring entering or leaving the panel should terminate on terminal blocks. The terminal blocks should be clearly identified with permanently marked terminal numbers and terminal block numbers. AC terminals should be 600-volt barrier terminal blocks, with screw clamp-type terminals, with or without pressure plates. Provide 25 percent spare terminals. Covers should be provided for terminals.

5.6.9.5 Panel Board Grounding

The panel must be grounded to the power ground bus for safety reasons. Conduits, trays, and the AC power supply grounds are connected to this ground. It is usual for a separate ground bus, insulated from the panel, to be mounted in the panel. Separate ground buses for AC and DC circuits offer a safeguard against feedback through the ground system from one instrument to another. In all cases, grounding practices must conform to *NEC* requirements and local governing codes.

5.6.10 INSTRUMENT AIR PIPING

Where instrument air is required, an air header is run to the control center or panel where it is valved and fitted with dual isolatable filter and regulator sets. Each set should be capable of handling the full air supply demand. The instrument air is reduced to 20 psig (140 KPa) for distribution to individual panels.

In each panel, a separate instrument air header should be mounted. These are mounted either vertically or sloped about 10 degrees from the horizontal. They should be provided with a drain valve at the low point. Each header should be capable of isolation from the main air supply. Each header should be fitted with valved takeoffs for each individual instrument requiring an instrument air supply. These may be valves or quick-disconnect pneumatic tube fittings. Materials used in panel instrument air systems should be brass, copper, aluminum, or galvanized steel.

COPYRIGHT 2002; American Petroleum Institute

Document provided by IHS Licensee=Sincor Venezuela/5934214100, User=, 08/13/2002 12:13:45 MDT Questions or comments about this message: please call the Document Policy Management Group at 1-800-451-1584.

API RP*554 95 ■ 0732290 0549623 374 ■

5.6.11 INSTRUMENT TUBING

Pneumatic instrument tubing systems located in panels are usually run from a bulkhead located at a point on the panel which is convenient for incoming field signal tubing terminations.

Each bulkhead point should be tagged with its instrument tag number.

Flexible tubing should be fire resistant, in which case it may be run in plastic or metal ducting mounted in the panel; or it may be copper or aluminum, in which case it would be bent to shape and self-supported. Tubing is usually ¼-inch outside diameter. Termination of tubing is usually achieved using tube compression fittings.

COPYRIGHT 2002; American Petroleum Institute

Document provided by IHS Licensee=Sincor Venezuela/5934214100, User=, 08/13/2002 12:13:45 MDT Questions or comments about this message: please call the Document Policy Management Group at 1-800-451-1584.

1-01400—9/95—7.5C (1E)

COPYRIGHT 2002; American Petroleum Institute

Document provided by IHS Licensee=Sincor Venezuela/5934214100, User=,
08/13/2002 12:13:45 MDT Questions or comments about this message: please call
the Document Policy Management Group at 1-800-451-1584.

American Petroleum Institute
1220 L Street, Northwest
Washington, D.C. 20005



Order No. C55401

COPYRIGHT 2002; American Petroleum Institute

Document provided by IHS Licensee=Sincor Venezuela/5934214100, User=,
08/13/2002 12:13:45 MDT Questions or comments about this message: please call
the Document Policy Management Group at 1-800-451-1584.