

The background of the cover features a complex industrial scene. It includes technical line drawings of pipes and machinery overlaid on a photograph of industrial equipment. The photograph shows large, perforated metal vessels, likely heat exchangers, connected by a network of pipes with several large blue handwheel valves. The overall color palette is a mix of light blues, greys, and the dark teal of the text overlay.

Practical Industrial Cybersecurity

ICS, INDUSTRY 4.0, AND IIoT

Charles J. Brooks
Philip A. Craig Jr.

WILEY

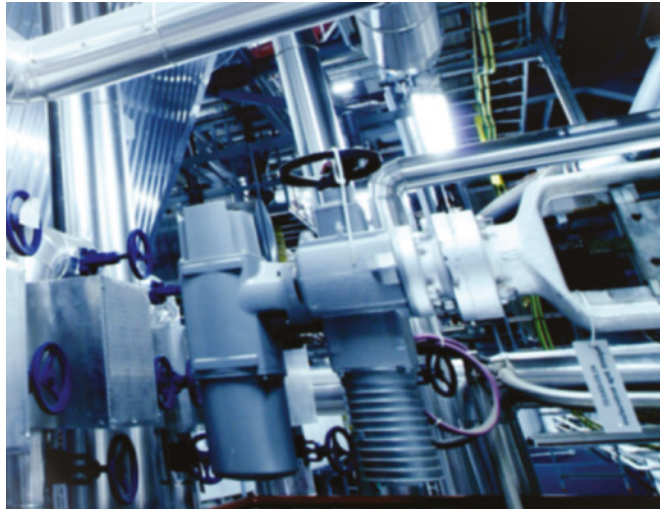
Practical Industrial Cybersecurity



Practical

Industrial Cybersecurity

ICS, Industry 4.0, and IIoT



Charles J. Brooks
Philip A. Craig Jr.

WILEY

Copyright © 2022 by John Wiley & Sons, Inc. Original drawings copyright © 2022, Educational Technologies Group Inc. All rights reserved.

Published by John Wiley & Sons, Inc., Hoboken, New Jersey.

Published simultaneously in Canada.

ISBN: 978-1-119-88302-9

ISBN: 978-1-119-88303-6 (ebk)

ISBN: 978-1-119-88304-3 (ebk)

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning, or otherwise, except as permitted under Section 107 or 108 of the 1976 United States Copyright Act, without either the prior written permission of the Publisher, or authorization through payment of the appropriate per-copy fee to the Copyright Clearance Center, Inc., 222 Rosewood Drive, Danvers, MA 01923, (978) 750-8400, fax (978) 750-4470, or on the web at www.copyright.com. Requests to the Publisher for permission should be addressed to the Permissions Department, John Wiley & Sons, Inc., 111 River Street, Hoboken, NJ 07030, (201) 748-6011, fax (201) 748-6008, or online at www.wiley.com/go/permission.

Limit of Liability/Disclaimer of Warranty: The publisher and the author make no representations or warranties with respect to the accuracy or completeness of the contents of this work and specifically disclaim all warranties, including without limitation warranties of fitness for a particular purpose. No warranty may be created or extended by sales or promotional materials. The advice and strategies contained herein may not be suitable for every situation. This work is sold with the understanding that the publisher is not engaged in rendering legal, accounting, or other professional services. If professional assistance is required, the services of a competent professional person should be sought. Neither the publisher nor the author shall be liable for damages arising herefrom. The fact that an organization or Website is referred to in this work as a citation and/or a potential source of further information does not mean that the author or the publisher endorses the information the organization or Website may provide or recommendations it may make. Further, readers should be aware the Internet Websites listed in this work may have changed or disappeared between when this work was written and when it is read.

For general information on our other products and services or for technical support, please contact our Customer Care Department within the United States at (800) 762-2974, outside the United States at (317) 572-3993 or fax (317) 572-4002.

Wiley also publishes its books in a variety of electronic formats. Some content that appears in print may not be available in electronic formats. For more information about Wiley products, visit our web site at www.wiley.com.

Library of Congress Control Number: 2022936106

Trademarks: WILEY and the Wiley logo are trademarks or registered trademarks of John Wiley & Sons, Inc. and/or its affiliates, in the United States and other countries, and may not be used without written permission. All other trademarks are the property of their respective owners. John Wiley & Sons, Inc. is not associated with any product or vendor mentioned in this book.

Cover image: © Andrei Merkulov / Adobe Stock

Cover design: Wiley

About the Authors

Charles J. Brooks is currently co-owner and vice president of Educational Technologies Group Inc., as well as co-owner of eITPrep LLP, an online training company. He is in charge of research and product development at both organizations.

A former electronics instructor and technical writer with the National Education Corporation, Charles taught and wrote on post-secondary ETG curriculum, including introductory electronics, transistor theory, linear integrated circuits, basic digital theory, industrial electronics, microprocessors, and computer peripherals.

Charles has authored several books, including seven editions of *A+ Certification Training Guide*, *The Complete Introductory Computer Course*, and *PC Peripheral Troubleshooting and Repair*. He also writes about green technologies, networking, residential technology integration, and IT convergence.

For the past eight years Charles has been lecturing and providing instructor training for cybersecurity teachers throughout the United States and abroad. His latest projects have been associated with IT and OT cybersecurity courses and hands-on lab activities and include Cybersecurity Essentials – Concepts & Practices; Cybersecurity Essentials – Environments & Testing; and Industrial Network Cybersecurity.

Philip A. Craig Jr. is the founder of BlackByte Cyber Security, LLC, a consultancy formed to develop new cybersecurity tools and tactics for use in US critical infrastructure. He oversees research and product development for the US Department of Energy (DOE), the Defense Advanced Research Projects Agency (DARPA), and the National Rural Electric Cooperative Association (NRECA), as well as providing expert knowledge in next-generation signal isolation techniques to protect automated controls in energy generation, transmission, and distribution systems. Mr. Craig has authored regulation for both the Nuclear Regulatory Commission (NRC) and the National Energy Reliability Corporation (NERC) and is an active cyber responder in federal partnerships for incident response.

About the Technical Editor

James R. McQuiggan, CISSP, SACP, is a security awareness advocate for KnowBe4. Prior to joining KnowBe4, McQuiggan worked for Siemens for 18 years, where he was responsible for various roles, including his most recent as the product and solution security officer for Siemens Gamesa Renewable Energy. In this role, he consulted for and supported various corporate divisions on cybersecurity standards, information security awareness, and securing product networks. In addition to his work at Siemens, McQuiggan is a part-time faculty professor at Valencia College in the Engineering, Computer Programming & Technology Division.

Within the Central Florida community, he is the president of the Central Florida (ISC)² chapter, where he supports cybersecurity professionals with education and networking opportunities.

Acknowledgments

Charles J. Brooks

First, I would like to thank Greg Michael, formerly of Howard W. Sams, for getting me involved in writing about microcomputer systems back in the early days of the IBM PC.

As always, I want to thank the staff here at ETG/Marcraft for making it easy to turn out a good product. In particular, thanks to Cathy Boulay and Luke Johns from the Product Development department for their excellent work in getting the text and lab books ready to go and looking good.

In addition, I would like to say thanks to Brian Alley of Dell Computers and Philip Craig, formerly of Pacific Northwest National Laboratory (PNNL) and now the owner of Black-Byte Cyber Security, LLC, for their expertise and guidance in bringing this group of books and their accompanying Lab Guides to fruition.

As always, I want to thank my wife, Robbie, for all of her understanding, support, and help with these projects, as well as Robert, Jamaica, Michael, and Joshua.

Philip A. Craig Jr.

To the folks who commit their lives and careers to developing new approaches to cybersecurity that protect the immense landscape of computing infrastructures from the malicious and sometimes deadly outcomes of cyberattacks, I dedicate this work to you. The next generation of cyber protectors will gain significant value from this book and hopefully will find its content sparking new dedication to the cyber challenges we will face in the years ahead.

I also dedicate this effort to my wife, Caralee, who has endured my long stays in our nation's capitol for many years, mostly for her understanding of the importance of my commitment to cybersecurity. As we celebrate her birthday on September 11 every year, we are reminded of what it means to our daily lives.

To the leadership at Marcraft, whose vision recognizes the value of teaching through hands-on experiences and not just text, thank you for recognizing and implementing your approach to our trade.

Contents at a Glance

<i>Introduction</i>		<i>xxiii</i>
Chapter 1	Industrial Control Systems	1
Chapter 2	ICS Architecture	43
Chapter 3	Secure ICS Architecture	95
Chapter 4	ICS Module and Element Hardening	143
Chapter 5	Cybersecurity Essentials for ICS	205
Chapter 6	Physical Security	271
Chapter 7	Access Management	315
Chapter 8	ICS Security Governance and Risk Management	347
Chapter 9	ICS Security Assessments	373
Chapter 10	ICS Security Monitoring and Incident Response	405
Chapter 11	Disaster Recovery and Business Continuity	453
Appendix A	GICSP Objective Map	481
Appendix B	Glossary	487
Appendix C	Standards and References	533
Appendix D	Review and Exam Question Answers	539
<i>Index</i>		<i>571</i>

Contents

Introduction

xxiii

Chapter 1	Industrial Control Systems	1
	Introduction	2
	Basic Process Control Systems	3
	Closed-Loop Control Systems	5
	Industrial Process Controllers	6
	Supervisory Control and Data Acquisition Systems	20
	System Telemetry	21
	Utility Networks	23
	OT/IT Network Integration	25
	Industrial Safety and Protection Systems	28
	Safety Instrument Systems	29
	Review Questions	39
	Exam Questions	41
Chapter 2	ICS Architecture	43
	Introduction	44
	Network Transmission Media	45
	Copper Cabling	45
	Fiber-Optic Cabling	46
	Industrial Network Media Standards	49
	Ethernet Connectivity	52
	External Network Communications	53
	Transmission Media Vulnerabilities	55
	Field Device Architecture	56
	PLC I/O Sections	58
	PLC Implementations	62
	Industrial Sensors	63
	Final Control Elements/Actuators	71
	Relays	73
	Process Units	76
	Industrial Network Protocols	79
	Common Industrial Protocols	79
	EtherNet/IP Protocol	79
	Modbus	80
	ProfiNet/ProfiBus	81
	DNP3	82
	ICCP	83

	OPC	83
	BACnet	83
	Enterprise Network Protocols	84
	TCP/IP	84
	Dynamic Host Configuration Protocol	89
	Review Questions	90
	Exam Questions	91
Chapter 3	Secure ICS Architecture	95
	Introduction	96
	Boundary Protection	97
	Firewalls	98
	Proxies	104
	Security Topologies	105
	Network Switches	106
	Routers	108
	Security Zoning Models	109
	Flat Network Topologies	113
	Network Segmentation	122
	Controlling Intersegment Data Movement	128
	Tunneling	128
	Wireless Networking	129
	Wireless Sensors	131
	Wireless Gateways	134
	Modems	135
	Review Questions	137
	Exam Questions	139
Chapter 4	ICS Module and Element Hardening	143
	Introduction	145
	Endpoint Security and Hardening	145
	User Workstation Hardening	145
	BIOS Security Subsystems	147
	Additional Outer Perimeter Access Hardening	148
	Mobile Device Protection	154
	OS Security/Hardening	155
	File System Security	156
	Operating System Security Choices	160
	Linux SystemV vs Systemd	160
	Hardening Operating Systems	162
	Common Operating System Security Tools	162
	Virtualization	169
	Application Software Security	172
	Software Exploitation	172
	Information Leakage	173

Applying Software Updates and Patches	174
Database Hardening	174
SQL Injection	175
Anti-Malware	177
Antivirus	178
Anti-spyware	178
Anti-Malware: Sanitization	181
Embedded Device Security	182
Meters	184
Network Hardening	189
OT/IT Network Security	189
Server Security	191
Hardening the Server OS	193
Logical Server Access Control	194
Hardening Network Connectivity Devices	196
Review Questions	201
Exam Questions	202

Chapter 5 Cybersecurity Essentials for ICS 205

Introduction	207
Basic Security Tenets	208
Confidentiality, Integrity, and Availability	208
Availability in ICS Networks	209
Nonrepudiation	210
Principle of Least Privilege	211
Separation of Duties	211
Vulnerability and Threat Identification	212
Nation-States	213
Cyberterrorists	213
Cybercriminals	214
Insider Threats	216
Events, Incidents, and Attacks	217
Threat Vectors	217
Weaponization	230
Delivery	230
Exploitation	231
Installation	232
Command and Control	233
Actions on Objectives	233
Attack Methods	234
Unauthorized Access	251
Cryptographics	260
Encryption	262
Digital Certificates	264

	Public Key Infrastructure	264
	Hashing	266
	Resource Constraints	267
	Review Questions	268
	Exam Questions	268
Chapter 6	Physical Security	271
	Introduction	272
	Infrastructure Security	273
	Access Control	274
	Physical Security Controls	276
	Authentication Systems	278
	Remote Access Monitoring and Automated Access Control Systems	286
	Intrusion Detection and Reporting Systems	289
	Security Controllers	290
	Video Surveillance Systems	295
	Cameras	297
	IP Cameras	297
	Pan-Tilt-Zoom Cameras	298
	Physical Security for ICS	306
	Industrial Processes/Generating Facilities	307
	Control Center/Company Offices	307
	NERC CIP-006-1	309
	Review Questions	311
	Exam Questions	312
Chapter 7	Access Management	315
	Introduction	316
	Access Control Models	317
	Mandatory Access Control	317
	Discretionary Access Control	318
	Role-Based Access Control	318
	Rule-Based Access Control	319
	Attribute-Based Access Control	319
	Context-Based Access Control	320
	Key Security Components within Access Controls	320
	Directory Services	321
	Active Directory	321
	Linux Directory Services	324
	Application Runtime and Execution Control	326
	User Access Management	326
	Establishing User and Group Accounts	328

	Group Account Security	330
	Network Authentication Options	331
	Establishing Resource Controls	332
	ICS Access Control	334
	Remote ICS Access Control	336
	Access Control for Cloud Systems	340
	Review Questions	343
	Exam Questions	344
Chapter 8	ICS Security Governance and Risk Management	347
	Introduction	348
	Security Policies and Procedure Development	348
	Requirements	349
	Exceptions and Exemptions	350
	Standards	351
	ICS Security Policies	356
	Risk Management	357
	Asset Identification	358
	Risk Assessment	359
	Risk Identification Vulnerability Assessment	362
	Impact Assessment	363
	ICS Risk Assessments	364
	Risk Mitigation	366
	NERC CIP-008	367
	Review Questions	369
	Exam Questions	370
Chapter 9	ICS Security Assessments	373
	Introduction	374
	Security Assessments	374
	ICS Device Testing	376
	Vulnerability	376
	Supply Chain	377
	Communication Robustness Testing	382
	Fuzzing	382
	ICS Penetration Testing	384
	The Pentest Process	385
	Security Testing Tools	392
	Packet Sniffers	392
	Network Enumeration/Port Scanning	393
	Port Scanning	395
	Vulnerability Scanning	395
	Review Questions	401
	Exam Questions	402

Chapter 10	ICS Security Monitoring and Incident Response	405
	Introduction	407
	ICS Lifecycle Challenges	408
	Change Management	408
	Establishing a Security Baseline	409
	Change Management Documentation	411
	Configuration Change Management	412
	Controlling Patch Distribution and Installation for Systems	414
	Monitoring	419
	Event Monitoring	420
	Network Monitoring	421
	Security Monitoring	423
	Logging and Auditing	424
	Event Logging	425
	Incident Management	433
	The Incident Response Lifecycle	434
	Preparation	435
	Incident Response	442
	Recovery	445
	Post-Incident Activities	446
	Review Questions	449
	Exam Questions	450
Chapter 11	Disaster Recovery and Business Continuity	453
	Introduction	454
	Business Continuity Plans	455
	System Redundancy	455
	Local Virtualized Storage	459
	System Backup and Restoration	462
	Backup Options	463
	Backup Media Rotation	466
	Securing Backup Media	467
	Other BCP Considerations	467
	Disaster Recovery	469
	Planning	470
	Documenting the Disaster Recovery Plan	472
	The Disaster Response/Recovery Team	473
	NERC CIP-009-6	475
	Review Questions	477
	Exam Questions	478
Appendix A	GICSP Objective Map	481
	ICS410.1 ICS: Global Industrial Cybersecurity Professional (GICSP) Objectives	482
	Overview	482

	ICS410.2: Architecture and Field Devices	483
	ICS410.3: Communications and Protocols	484
	ICS410.4: Supervisory Systems	485
	ICS410.5: Security Governance	485
Appendix B	Glossary	487
Appendix C	Standards and References	533
	Reference Links	536
Appendix D	Review and Exam Question Answers	539
	Chapter 1: Industrial Control Systems	540
	Review Question Answers	540
	Exam Question Answers	541
	Chapter 2: ICS Architecture	542
	Review Question Answers	542
	Exam Question Answers	544
	Chapter 3: Secure ICS Architecture	545
	Review Question Answers	545
	Exam Question Answers	547
	Chapter 4: ICS Modules and Element Hardening	548
	Review Question Answers	548
	Exam Question Answers	550
	Chapter 5: Cybersecurity Essentials for ICS	551
	Review Question Answers	551
	Exam Question Answers	553
	Chapter 6: Physical Security	554
	Review Question Answers	554
	Exam Question Answers	556
	Chapter 7: Access Management	556
	Review Question Answers	556
	Exam Question Answers	558
	Chapter 8: ICS Security Governance and Risk Management	559
	Review Question Answers	559
	Exam Question Answers	560
	Chapter 9: ICS Security Assessments	561
	Review Question Answers	561
	Exam Question Answers	563
	Chapter 10: ICS Security Monitoring and Incident Response	564
	Review Question Answers	564
	Exam Question Answers	565
	Chapter 11: Disaster Recovery and Business Continuity	567
	Review Question Answers	567
	Exam Question Answers	568
	<i>Index</i>	571

Foreword

Imagine waking up in a house one day with no electricity. Or maybe your gas heater won't turn on, or you have no water flowing to your house. Simple everyday conveniences? No, these resources are critical dependencies that provide health, safety, nourishment, and general stability and security—not only in our homes and businesses but throughout society as a whole. These are exactly the outcomes of a coordinated cyberattack against critical infrastructure. Now imagine this type of cyber event on a national scale. We should all be concerned about this type of cyber event, not only regarding these basic necessities, but concerning stability if our financial or healthcare services are compromised. We are at an unbalanced period of cyberthreats versus our ability to identify and react to cyberattacks on this type of scale.

A few years ago, I had the pleasure of working with the coauthor of this book, Mr. Phil Craig Jr. Together we provided our skills to support a critical electric infrastructure security program sponsored by the Defense Advanced Research Projects Agency (DARPA). The project explored and developed cybersecurity tools to quickly recover the US electrical grid from a persistent and aggressive cyberattack that would severely impact the stability of a large-scale power grid. We learned that the threats were real, and the challenge could be overwhelming.

Understanding, operating, and defending the digital environments that provide stable controls and communications in a highly connected environment are paramount tasks when preventing the cyber events we fear will affect our daily lives. Mr. Craig and his colleagues have amassed years of experience in the evolution of operational technology systems and in creating technology to identify and mitigate cyberthreats in them, and Mr. Charles Brooks has been a significant contributor to exceptional “hands-on” training techniques and materials for many years. With their combined knowledge, the book provides a perspective of how immense the opportunity is for cyber intrusions and attacks and introduces impactful techniques to increase cyber defenses against them. Both Mr. Brooks's and Mr. Craig's technical acumen are surpassed only by their passion for educating new generations of cyber defenders to protect these essential systems and networks from those who try to alter our way of life.

This book is a useful resource for both newcomers and experienced individuals who are attempting to broaden their knowledge of industrial control systems and cybersecurity countermeasures as cyberthreats continue to grow. The book strongly supports and identifies critical skills that are desperately needed to provide protective measures to counter these threats. It is logically organized and provides references for technicians working in the OT trade and attempting certification as Global Industrial Cyber Security Professionals (GICSPs). Finally, this book provides a comprehensive resource for any cybersecurity professional who desires to expand their breadth of security knowledge on the latest cyber techniques used in the industry.

Mr. Joseph Minicucci
Lt. Col USMC

Introduction

Welcome to Wiley's *Practical Industrial Cybersecurity: ICS, Industry 4.0, and IIoT*. This book is designed to provide a solid theory and practical platform for cybersecurity personnel in the industrial process control and utility environments.

While this book does not stand on its own as a complete guide to becoming an industrial cybersecurity professional, it does prepare readers to prepare for the leading industry certification in this area—the Global Industrial Cyber Security Professional (GICSP) exam from Global Information Assurance Certification (GIAC), an affiliate of the SANS Institute. The GICSP exam is designed to bring industrial control skills to the cybersecurity forefront. While there are multitudes of IT-centric computer, network, and cybersecurity courses and certifications in the field, there are not many individuals who possess the skills and knowledge of cybersecurity as it relates to industrial control systems and operations technology. The search for people with these skills and knowledge has becoming a driving force in the cybersecurity world.

The published topic areas for each GICSP Exam Certification Objectives & Outcome Statements are as follows:

- Access Management—Knowledge of access control models, directory services, and user access management
- Configuration/Change Management—Knowledge of change management, baselines, equipment connections, and configuration auditing
- Configuration/Change Management—software updates—Knowledge of distribution and installation of patches, knowledge of software reloads and firmware management
- Cybersecurity Essentials for ICS—Knowledge of attacks and incidents (e.g., man in the middle, spoofing, social engineering, denial of service, denial of view, data manipulating, session hijacking, foreign software, unauthorized access)
- Cybersecurity Essentials for ICS—Knowledge of availability (e.g., health and safety, environmental, productivity)
- Cybersecurity Essentials for ICS—Knowledge of cryptographics (e.g., encryption, digital signatures, certificate management, PKI, public versus private key, hashing, key management, resource constraints)
- Cybersecurity Essentials for ICS—Knowledge of security tenets (e.g., CIA, non-repudiation, least privilege, separation of duties)
- Cybersecurity Essentials for ICS—Knowledge of threats (e.g., nation-states, general criminals, inside and outside malicious attackers, hacktivists, inside non-malicious)
- Disaster Recovery and Business Continuity—Knowledge of system backup and restoration
- ICS Architecture—Knowledge of communication medium and external network communications

- ICS Architecture—Knowledge of field device architecture (e.g., relays, PLC, switch, process unit)
- ICS Architecture—Knowledge of industrial protocols (e.g., Modbus, Modbus TCP, DNP3, Ethernet/IP, OPC)
- ICS Architecture—Knowledge of network protocols (e.g., DNS, DHCP, TCP/IP)
- ICS Architecture—Knowledge of network segmentation (e.g., partitioning, segregation, zones and conduits, reference architectures, network devices and services, data diodes, DMZs)
- ICS Architecture—Knowledge of wireless security (e.g., Wi-Fi, wireless sensors, wireless gateways, controllers)
- ICS Modules and Element Hardening—Knowledge of application security (e.g., database security)
- ICS Modules and Element Hardening—Knowledge of embedded devices (e.g., PLCs, controllers, RTUs, analyzers, meters, aggregators, security issues, default configurations)
- ICS Modules and Element Hardening—Knowledge of network security/hardening (e.g., switchport security)
- ICS Modules and Element Hardening—Knowledge of OS security (Unix/Linux, Windows, least privilege security, virtualization)
- ICS Modules and Element Hardening—Configuration and endpoint hardening—knowledge of anti-malware implementation, updating, monitoring, and sanitization. Knowledge of endpoint protection including user workstations and mobile devices
- ICS Security Assessments—Knowledge of security testing tools (e.g., packet sniffer, port scanner, vulnerability scanner)
- ICS Security Assessments—Assessments and testing—knowledge of device testing (e.g., communication robustness, fuzzing) (e.g., risk, criticality, vulnerability, attack surface analysis, supply chain), penetration testing and exploitation, security assessment
- ICS Security Governance and Risk Management—Knowledge of risk management (e.g., PHA/HAZOP usage, risk acceptance, risk/mitigation plan)
- ICS Security Governance and Risk Management—Knowledge of security policies and procedures development (e.g., exceptions, exemptions, requirements, standards)
- ICS Security Monitoring—Knowledge of event, network, and security logging, including knowledge of archiving logs
- ICS Security Monitoring—Knowledge of event, network, and security monitoring
- Incident Management—Knowledge of incident recognition and triage (e.g., log analysis/event correlation, anomalous behavior, intrusion detection, egress monitoring, IPS), knowledge of incident remediation/recovery, and knowledge of incident response (e.g., recording/reporting, forensic log analysis, containment, incident response team, root cause analysis, eradication/quarantine)

- Industrial Control Systems—Knowledge of basic process control systems (e.g., RTU, PLC, DCS, SCADA, metering/telemetry, Ethernet I/O, buses, Purdue [ISA 95])
- Industrial Control Systems—Knowledge of safety and protection systems (e.g., SIS, EMS, leak detection, FGS, BMS, vibration monitoring)
- Physical Security—Knowledge of physical security

Additional information about the GICSP exam is presented in Appendix A.

What Does This Book Cover?

This book prepares readers to prepare for the leading industry certification in this area—the Global Industrial Cyber Security Professional (GICSP) exam from Global Information Assurance Certification (GIAC), an affiliate of the SANS Institute.

The *Practical Industrial Cybersecurity: ICS, Industry 4.0, and IIoT* book is a basic training system designed to provide a solid understanding of industrial cybersecurity challenges, tools, and techniques, as well as to develop the foundations of a professional cybersecurity skill set. This is accomplished in a progressive process, as follows:

Chapter 1: Industrial Control Systems

Unless you've been working in an industrial process environment, the operations, devices, protocols, and standards involved in those types of environments are probably foreign to you. This initial chapter is designed to introduce the reader to the functions of components and systems involved in basic industrial process control operations. The latter sections of the chapter address common industrial safety and protection systems.

Chapter 2: ICS Architecture

For individuals acquainted with typical enterprise/IT networking, an industrial network is still an alien environment in many ways. Even the most basic components and tenets of operating an OT network are different from those found in a traditional IT network. This chapter presents the reader with an introduction to basic OT field device architecture and contrasts the basic functions of common industrial and enterprise network protocols.

Chapter 3: Secure ICS Architecture

This chapter builds on the basic information introduced in the preceding chapter to show how those components are organized to produce secure operational technology (OT) network architecture. This involves two major topic areas—network segmentation and security zoning as well as wireless network security.

Chapter 4: ICS Modules and Element Hardening

Industrial network security efforts begin with hardening hardware. However, it also extends to the local host's operating system, its file system, and its applications. This chapter covers

techniques and practices involved in OT module and element hardening in six major areas—endpoint protection, embedded device security, OS security, application security, and use of anti-malware products in IT and OT networks as well as network security/hardening efforts.

Chapter 5: Cybersecurity Essentials for ICS

The opening sections of this chapter deal with the most fundamental cybersecurity tenets—CIA, AAA, nonrepudiation, the principle of least privilege, and separation of duties policies. Unlike in the typical IT network environment, data confidentiality is not usually the top security tenet associated with OT networks. Instead, the most important tenet is typically availability. ICS networks are real-time environments, and having data available in real time is usually more important than its confidentiality.

The middle sections of the chapter turn to address the knowledge of threats to industrial/utility environments. This includes descriptions of the different players involved in cybersecurity realms, as well as the nature of different types of attacks conducted against them.

The final sections of the chapter deal with employing cryptographic techniques to encrypt and protect data. Information covered in these sections includes digital signatures, certificate management, PKI, public/private keys, hashing, and key management.

Chapter 6: Physical Security

The beginning of all security is physical security. Even though it is often not mentioned in the same text as computer, network, or cybersecurity, those forms of security cannot exist without physical security. This chapter defines physical security and examines how infrastructure security fits into cybersecurity. The information in this chapter will enable readers to differentiate between authentication and authorization, identify typical physical access control devices, and identify strengths and weaknesses of different types of security and surveillance systems and devices.

Chapter 7: Access Management

Access control is basically a strategy for identifying people doing specific jobs, authenticating them through some type of identification system, and then giving only them keys to the assets they need access to. The previous chapter addressed this at the physical level. This chapter deals with logical access control models and practices associated with controlling access in enterprise and OT networks. Key topics here include coverage of typical directory services and user access management procedures and policies.

Chapter 8: ICS Security Governance and Risk Management

Policies, procedures, and guidelines are governance elements that work together to provide employees with adequate guidance to perform their tasks within an organization. This chapter examines these elements and how they are developed to meet the needs of the organization. Key ICS topics developed here include standards, requirements, exemptions, and exceptions.

The chapter also deals with how organizations manage risk in the development, deployment, and maintenance of their policies and procedures. This includes calculating and

evaluating risk factors to determine risk mitigation and risk acceptance strategies. When an organization undertakes an OT security assessment, risk mitigation, and security policy generation plan, they must address certain areas of risk. You will be introduced to standard risk management tools used in the ICS network environment, such as risk mitigation plans and PHA Hazard and Operability (HAZOP) studies.

Chapter 9: ICS Security Assessments

A security assessment involves testing the network architecture and its policies, procedures, and guidelines in a realistic way to determine its effectiveness. This chapter discusses penetration testing and exploitation in the OT network environment. This includes becoming familiar with security testing tools and the ICS device testing strategies involved in security assessments. You will be introduced to security assessment exercises designed to locate vulnerabilities within an organization's network and computing environment.

Chapter 10: ICS Security Monitoring and Incident Response

After the research has been conducted, the network has been designed and implemented, and the security assessment has been conducted and validated, continued security must be provided by monitoring and auditing the network for activities that indicate it is being threatened or has already been compromised. This chapter addresses ongoing security in the form of event, network, and security monitoring and logging activities. Key topics related to these efforts include change management, distribution and installation of patches, software reloads, and firmware management.

The second half of the chapter examines the implementation of an effective incident response plan. In modern networks of all kinds, it is naive to think that any of them will not be attacked—it's not if, it's when. The key to successfully managing these events is having a well-developed and tested incident response plan and being knowledgeable of incident recognition, triage, and remediation/recovery steps and techniques.

Chapter 11: Disaster Recovery and Business Continuity

Organizations must be able to continue operations despite all types of small emergencies and large disasters to ensure the health and continuation of the organization. This involves looking ahead and creating a robust disaster recovery plan and business continuity plan. This chapter examines best practices associated with creating these two interrelated documents.

The book concludes with discussions of how to recover from a successful attack or natural disaster. The best solution for these types of events is having the ability to recover quickly and get back to partial and then full operations. This section discusses different system backup and restoration options and practices.

An abundance of assessment material is available with this book. At the end of each chapter are 15 open-ended/fill-in-the-blank questions and 10 multiple-choice questions. The 10 multiple-choice questions test your knowledge of the basic concepts presented in the chapter, while the 15 open-ended questions are designed to test comprehension and critical thinking.

Appendix A contains information specific to enrolling and taking the GICSP exam from GIAC. The scope and sequencing of this course was developed from the objectives list of the Global Industrial Cyber Security Professional (GICSP) exam.

Appendix B contains an extensive glossary of GICSP terms.

Appendix C contains key references used in the development of this book and are provided to give you a source of materials to round out the topics covered here.

Reader Support for This Book

We provide email addresses for reader support in the following sections.


How to Contact the Publisher

If you believe you've found a mistake in this book, please bring it to our attention. At John Wiley & Sons, we understand how important it is to provide our customers with accurate content, but even with our best efforts an error may occur.

To submit your possible errata, please email it to our Customer Service Team at wileysupport@wiley.com with the subject line "Possible Book Errata Submission."

How to Contact the Author

We appreciate your input and questions about this book! Email me at chuckb@marcraft.com.

A vertical image on the left side of the page showing an industrial setting with large pipes, valves, and machinery. The text 'Chapter 1' is overlaid on the top left of this image.

Chapter 1

Industrial Control Systems

OBJECTIVES

Upon completion of this chapter, you should be able to:

1. Describe the functions of components and systems involved in basic industrial process control operations, including:
 - Closed loop
 - RTU
 - IED
 - PLC
 - DCS
 - SCADA
 - Metering/telemetry
 - Ethernet I/O
 - Bus (field)
 - Purdue (ISA 95)
2. Describe common industrial safety and protection systems, including:
 - SIS
 - EMS
 - Leak detection
 - FGS
 - BMS
 - Vibration monitoring



Introduction

In general, people everywhere are becoming more aware of how interactions involving inter-networked systems can affect their personal and financial security. However, we tend to be less aware of how security issues associated with the critical industrial processing and utility services infrastructure involve us. These critical infrastructure sectors include the following:

- Industrial processing
 - Manufacturing
 - Chemical processing
 - Agriculture
- Utility services
 - Water
 - Electricity
 - Wastewater
 - Oil and gas
 - Transportation

Consider the areas called out in these two sectors and think about how much of your life would be impacted if any of these critical infrastructure sectors became severely damaged or disabled by a security event. Then consider that most participants in both infrastructure sectors have increased their usage of cyber technologies to make their operations more automated, efficient, and productive. In doing so, they have exposed their operations to the same types of cybersecurity threats that are associated with personal and organizational networks.

While cybersecurity policies and practices for industrial and utility organizations seem similar to those associated with enterprise network security, they are quite different in application. Personnel trained in enterprise network security may see only a passing similarity to the networks they are familiar with if they were introduced to an industrial or utility network environment.

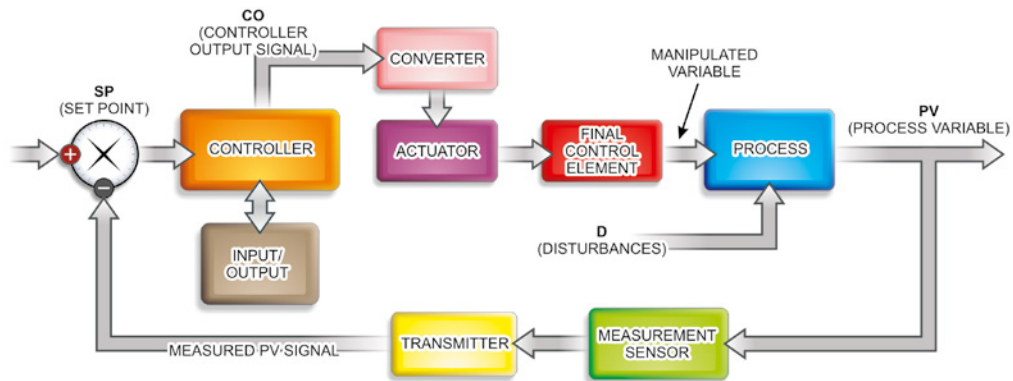
It's not as though there are no transferable skill and knowledge sets between IT networks and industrial/utility network environments. In fact, as you read this book, we will blend

basic organizational IT networking information with new information you will need to understand to be successful in the industrial/utility network security environment.

Basic Process Control Systems

The basis of all industrial production and utility services operations is the implementation of automated process control systems. Let's begin by examining the basic elements associated with any industrial process control system. Figure 1.1 depicts a generic automated process in block diagram format.

FIGURE 1.1 Blocks of an automated process



Within the block labeled “process” is some variable such as temperature, pressure, flow rate, level, rotational speed, or position that needs to be regulated. Any physical parameter that can change spontaneously or from external influences is a dynamic variable. A *dynamic variable* that is being controlled by the controller block is more specifically referred to as the *process variable (PV)*.

The overall objective of process control is to cause the PV to remain at some specific predetermined value referred to as the *set point (SP)*. The SP may be a fixed reference, such as a simple liquid level sensor mounted on a post, or it can be an adjustable reference like a common thermostat where the user can set a desired temperature to be maintained.

Because the PV is dynamic, the overall control system must constantly sample the state of the variable, compare it to the set point, and apply any corrective actions needed to maintain the PV at the desired SP. The devices that gather information about the system are collectively referred to as *input transducers* or *sensors*.

The output of the sensor may feed directly into the controller block, or this might be accomplished with an optional block titled “transmitter.” If the sensor is located at some

distance from the controller or its output is simply incompatible with the controller's input, an *interface* device must be used to convert the transducer's output signal to a signal that is better suited for transmission or that is compatible with the controlling device.

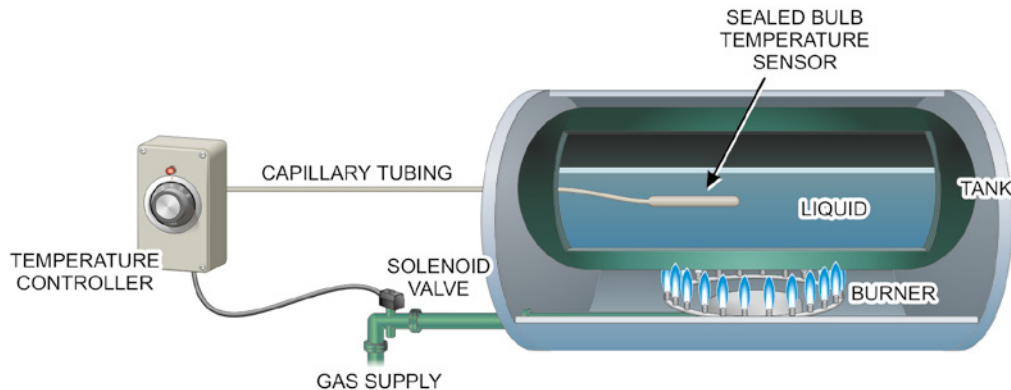
The heart of any process control system is the block marked “controller.” The controller is responsible for taking the input information, comparing that information to a predetermined condition or a reference, making decisions about what action should be taken, and finally sending corrective *error signals* to the final element, which adjusts the *manipulated variable*. Industrial control units may consist of magnetic relays, a collection of digital integrated circuits, analog electronic circuitry, pneumatic devices, microprocessors, or some combination of these devices.

Operator settings and system status information are entered and obtained from the block titled “Input/Output” or “I/O.” The I/O block may be an integral part of the controller or located at some remote location. A portion of the I/O block may be dedicated to displays and control mechanisms that enable a human operator to interact with the control system.

The correction signal issued from the controller may be applied directly to the *actuator* block or to an optional output signal converter that is used to make the controller's output signal compatible with the actuator. The task of the actuator is to apply the corrective action necessary to regulate the process variable to the established set point. Typical industrial control actuators are devices such as electric motor starters and pneumatic or solenoid-activated valves.

To understand how these elements work together to provide process control, consider the simple temperature control system depicted in Figure 1.2. This example depicts a control system that employs a liquid-filled sensing device, a simple set of electrical switch contacts, and an electrically operated solenoid gas valve.

FIGURE 1.2 A simple temperature control system



In the example in Figure 1.2, the PV (liquid temperature) is constantly monitored by the fluid in the sealed bulb and capillary tubing. As temperature increases in the enclosure, the

fluid expands in the bulb and tubing, causing it to press against a diaphragm at the end of the tubing. The movement of the diaphragm in turn pushes against one of a pair of electrical switch contacts, causing it to move closer to the other contact.

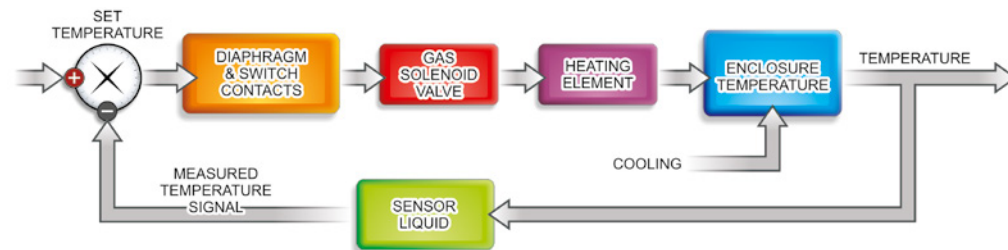
When the temperature in the enclosure reaches a predetermined level established by the sensor fluid's coefficient of expansion and the distance between the switch contacts, the contacts will go closed, creating an electrical circuit that activates a solenoid control valve. The electromagnet in the valve creates an electromagnetic field that pulls the valve stem upward, sealing off the flow of gas (the manipulated variable) to the heating element inside the enclosure (the final element).

The removal of the heat source will cause the temperature inside the enclosure to decrease until the bulb contracts and pulls the diaphragm away from the switch contacts. When this occurs, the contacts will open, cutting off the flow of electricity to the solenoid. The valve will open, and gas will once again flow into the heating element, causing the temperature to increase again.

Closed-Loop Control Systems

This simple temperature control system is a type of process control referred to as *closed-loop* control. As the block diagram in Figure 1.3 shows, there is a *feedback* pathway from the output of the process (temperature of the enclosure) that feeds back to the controller (the diaphragm and switch contacts), which then applies appropriate corrective action to the process input (the pneumatic gas valve and burner).

FIGURE 1.3 Closed-loop process blocks



The feedback loop through the controller enables the closed-loop system to be self-adjusting. The controller examines the measured process variable and compares it to the set point reference (in the earlier example the reference point was the position of the fixed-switch contact). It then creates an error response based on the outcome of the comparison.

Typically, if the process variable value is higher than the reference's value, a positive action is created, such as applying more gas to the heating element. Conversely, if the process variable value is equal to or higher than the reference value, the controller will produce a negative corrective action, such as shutting off the gas flow to the heating element.

In the example in Figure 1.3, the process control mode is simply On/Off: the valve is either completely open or completely closed. However, if analog output devices and input sensors are employed and the controller is intelligent (it has advanced decision-making capabilities such as a microprocessor-based controller), the closed-loop system can be built and configured to provide smooth, accurate, and sensitive control responses. These systems are the basis for all automated process control systems.

Industrial Process Controllers

As already discussed, the center of any process control system is its controller. Historically, process controllers have been based on a number of different technologies, including mechanical devices, pneumatic devices, analog electronics, discrete digital electronics, or microprocessor-based computer electronics. However, currently most process controllers are built on some type of microprocessor-based computer control technology.

While *industrial process controllers (IPCs)* share many qualities with microprocessor-based computing devices designed for the *information technology (IT)* industry (personal computers and network servers), they are very different in many ways. Unlike IT computers, industrial process controllers are not designed to store data and process it later. Instead, they produce output conditions based on the current states of their inputs according to their internal configuration or programming.



Industrial control systems are designed to control variables in the physical world, while IT systems are designed to manage data.

The following are key requirements for industrial process controllers:

- **Availability:** Many processes are continuous operations and require that the controller have high availability, reliability, and maintainability ratings. Availability is typically the highest objective in an industrial control system, along with data integrity. Confidentiality has traditionally been a secondary concern with process control systems; this is completely reversed from the general confidentiality, integrity, and availability (CIA) requirements associated with IT systems.
- **Timeliness:** Process control is a time-sensitive operation that requires quick response times. IT systems generally do not have timeliness constraints. For this reason, front-line intelligent process controllers operate on real-time operating systems.
- **Industrial interfacing:** Industrial controllers typically provide few if any user-friendly interface features, such as keyboards, pointing devices, or LCD displays. Instead, they provide industrial-style input and output ports for connecting sensors and actuators.
- **Physical hardening:** IPCs are designed to operate in harsh environments such as industrial factories and open air venues.

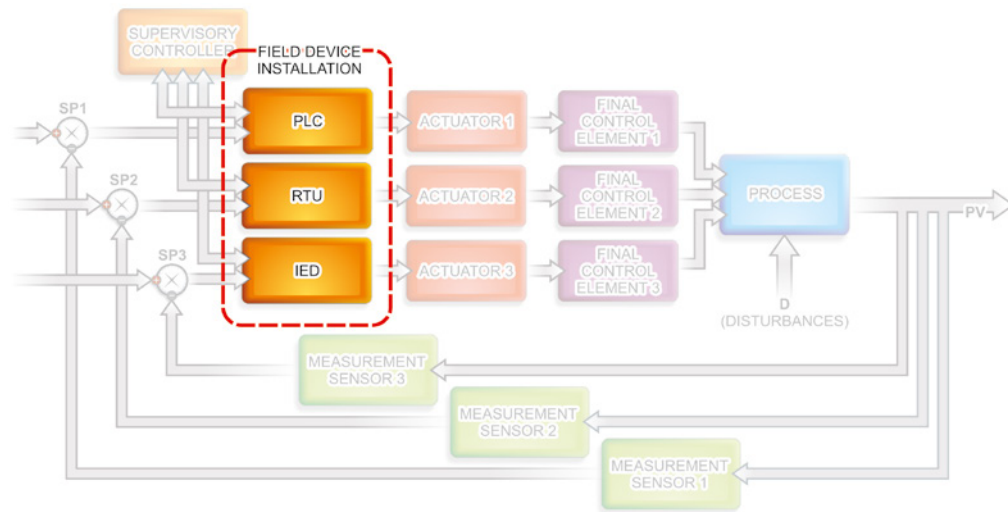
Field Devices

Industrial controllers that are designed to be deployed in close proximity to the process being controlled, as opposed to supervisory computing devices that are more routinely placed in an office or control room environment, are referred to as *field devices*. These are the most common field devices encountered in industrial and utility process control systems:

- Programmable logic controllers (PLCs)
- Remote telemetry units (RTUs)
- Intelligent electronic devices (IEDs)

In a dedicated control system, the field device or devices are placed between the sensors that gather information from the physical process and the actuators that supply corrective actions to the physical process. However, in a distributed control system, the field devices are logically located between the sensors and actuators and the supervisory control system with its human machine interfaces. Figure 1.4 shows how field devices are typically implemented in industrial control systems.

FIGURE 1.4 Field device implementations

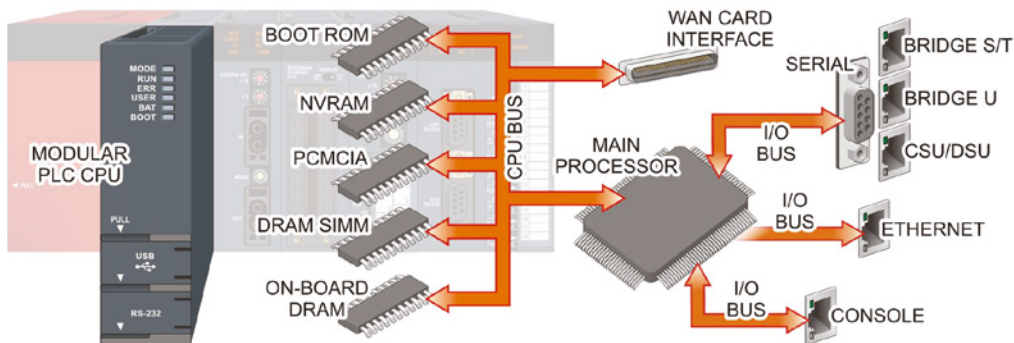


Programmable Logic Controllers

The preferred local control device in modern industrial processing and utility environments is the *programmable logic controller*, or PLC. PLCs are intelligent digital computing devices that are designed specifically to perform industrial control functions, such as opening and closing valves, switches, and relays to control processes.

Internally, PLCs like the one depicted in Figure 1.5 share most of their technology with IT computing devices. They contain a microprocessor, RAM memory, read-only firmware, and an operating system. However, this is where the similarities end.

FIGURE 1.5 A typical PLC



Because they are intelligent, PLC operation can be changed simply by reprogramming them with new instructions. PLCs use a programming method designed to resemble the *relay ladder logic* (because PLCs were originally designed to replace relay controllers that were widely used before digital processors were developed). These diagrams are discussed in Chapter 2, “ICS Architecture.” Newer PLCs can be programmed in many different ways, including through popular computer programming languages.

Programming can be downloaded or entered directly into the PLC’s programmable RAM area. PLC instruction sets can be used to implement specific control functions such as counting and timing loops; three-mode proportional, integral, derivative (PID) control; arithmetic operations; and I/O control. Programming can be accomplished through a programming interface installed on a local host computer.

PLC inputs are connected to sensors—temperature, pressure, or positional switches—that monitor process variables. On the other side of the equation, the PLC’s output terminals are attached to actuators—relays, solenoid valves, or mechanical positioners—which are devices used to control process variables, as illustrated in Figure 1.6.

The figure depicts a *point-to-point wiring* scheme for a PLC and its sensors and actuators. It also indicates that individual connections between the PLC and its devices can be made through wiring racks and junction boxes located throughout the production plant. However, each device is connected to an input or output terminal by a dedicated run of cable.

PLCs are available in different form factors including compact devices and modular units connected via a *backplane* system and housed in a common *rack*. Figure 1.7 depicts a typical compact PLC. It is a self-contained processing unit that offers input terminals along its top edge, output terminals along its bottom edge, and a power supply connection at its lower-left corner. The figure also illustrates that this PLC model makes provisions for connecting it to other devices through its serial communications terminals, as well as through a traditional Ethernet network connection.

FIGURE 1.6 PLC controlling a process

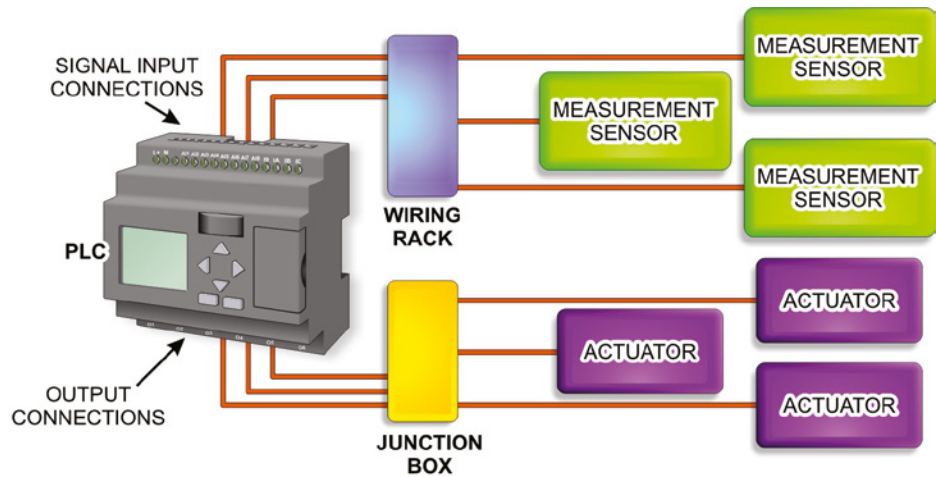
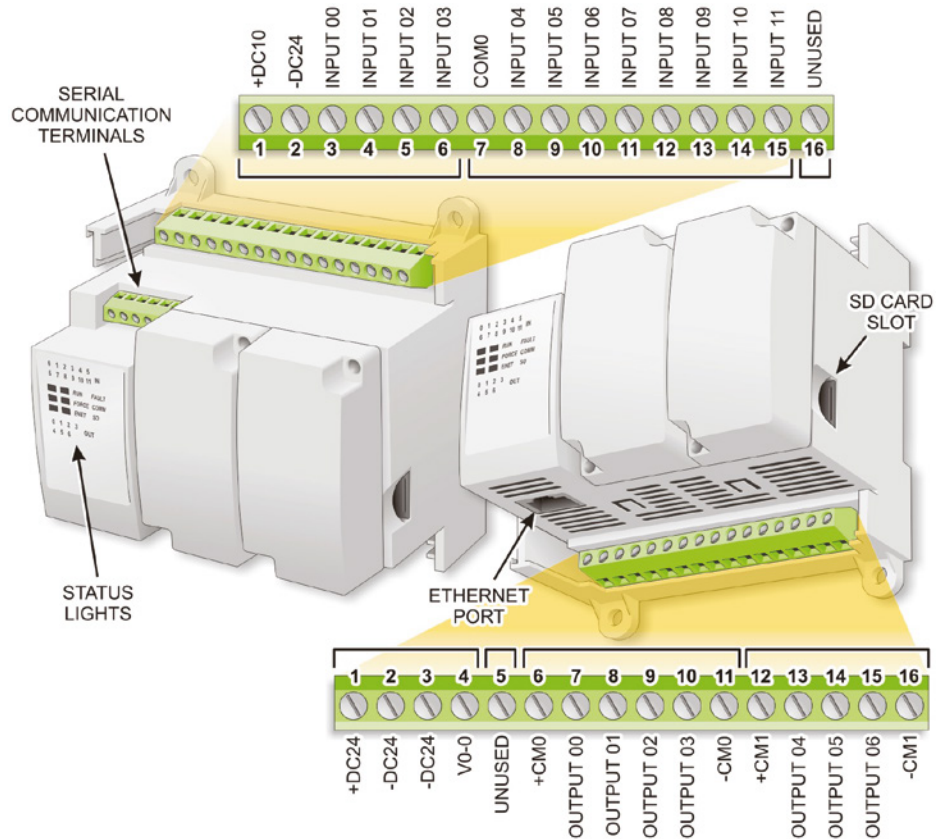
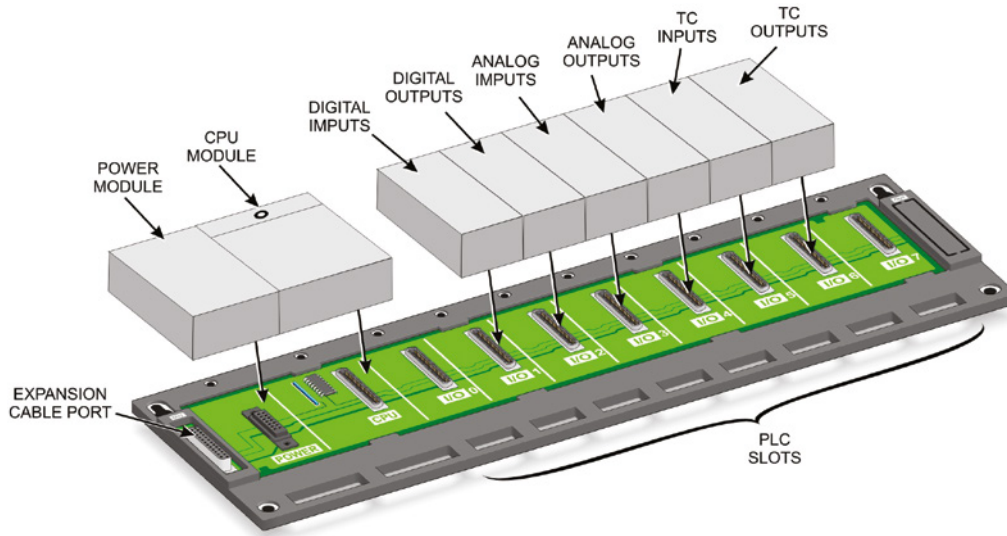


FIGURE 1.7 A typical compact PLC



Modular form-factor PLCs offer flexible input and output configurations, as multiple input or output modules can be added to the backplane. Figure 1.8 shows a typical PLC rack and backplane. The backplane is a printed circuit board that provides a common data bus and a series of slot connectors for connecting different modules to the system. One of the slot connectors is reserved for a power supply module. The other slot connectors (eight of them in this example) are designed to accept the CPU module and different types of I/O modules.

FIGURE 1.8 Modular PLC rack and backplane



Common PLC module types include the following:

- *Power supply unit (PSU) module:* This unit supplies power to the CPU and I/O modules through the backplane bus. PLC power supplies typically furnish 24Vac power to its components.
- *Central processing unit (CPU) module:* This is the PLC equivalent of the personal computer's motherboard. It contains the microprocessor, RAM and ROM memory, I/O interfacing circuitry, and communications support.
- *Input modules:* There are two basic types of input modules that can be installed in the PLC rack: analog input modules and digital input modules.
 - *Analog inputs:* Analog input modules are designed to operate with sensing devices, such as thermocouples and pressure sensors, that produce a continuously variable range of output values between a minimum and maximum (such as 0–10V). Because microprocessor-based control devices do not understand analog signals, the modules

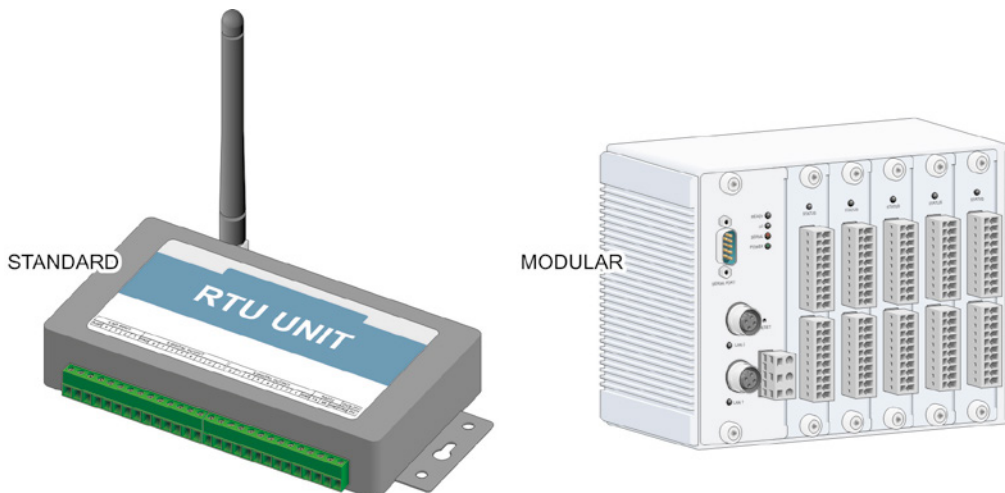
must perform an A/D conversion process on the signal to achieve a digital equivalent of the measured analog value that the CPU can work with.

- **Digital inputs:** This type of module is used to handle discrete digital input devices such as limit switches, photo/optical switches, proximity switches, and any other device that provides a two-state output. These modules are available to handle from 8 up to 128 devices.
- **Output modules:** Like input modules, output modules come in two basic varieties, analog and digital.
 - **Analog outputs:** These outputs provide analog signals that can be used to drive analog actuators, such as valve positioners. To produce this type of output signal, the module must perform a D/A conversion process on the values received from the CPU before they can be applied to the output terminals.
 - **Digital outputs:** These modules provide On/Off output signals for controlling two position actuators. Like digital input modules, digital output modules are available that can supply from 8 to 128 different output connections.
- **Comm modules:** These are communication modules that allow the CPU to communicate with other intelligent devices across the backplane's I/O bus. This has historically been done through standard asynchronous serial communication protocols such as RS-232 and RS-485 channels. However, newer industrial communications options are being introduced to the PLC communications, including different IT and telephony-based protocols, such as TCP/IP communication over Ethernet, Bluetooth, and Zigbee.

Remote Telemetry Units

Another common industrial controller is the *remote telemetry unit*, commonly referred to simply as an *RTU*. RTUs are small intelligent control units deployed at selective locations within a process, or set of processes, to gather data from different sensors and deliver commands to control relay outputs. Figure 1.9 shows a typical RTU.

FIGURE 1.9 An RTU controller





Telemetry is the process of using sensors to collect information in a remote location and transmitting it to another location for processing.

Like PLCs, RTUs can employ digital or analog input sensor devices designed to measure variables such as electrical currents and voltages, pressure, light levels, flow rates, fluid levels, turbidity, pH, rotary speed, etc. The analog inputs accept input signals from sensors within a given range. Common analog input signal ranges include 0 to 1mA or 4 to 20mA current ranges, or 0 to 10Vdc ranges, as well as $\pm 2.5\text{V}$ or $\pm 5.0\text{V}$ ranges. For sensor types that produce signal ranges outside of these parameters, some type of signal level translating interface device must be installed between the sensor and the input port. These industry-standard signaling methods and ranges are selected by different equipment manufacturers based on sensors used in different applications.

Voltage signaling is used in many sensor applications because it is relatively simple to implement. However, voltage signaling is susceptible to electrical noise interference and transmission distance limitations. Current signaling standards have historically been the accepted method of transporting sensor information because their response is more linear than voltage signaling methods as well as providing greater noise immunity.

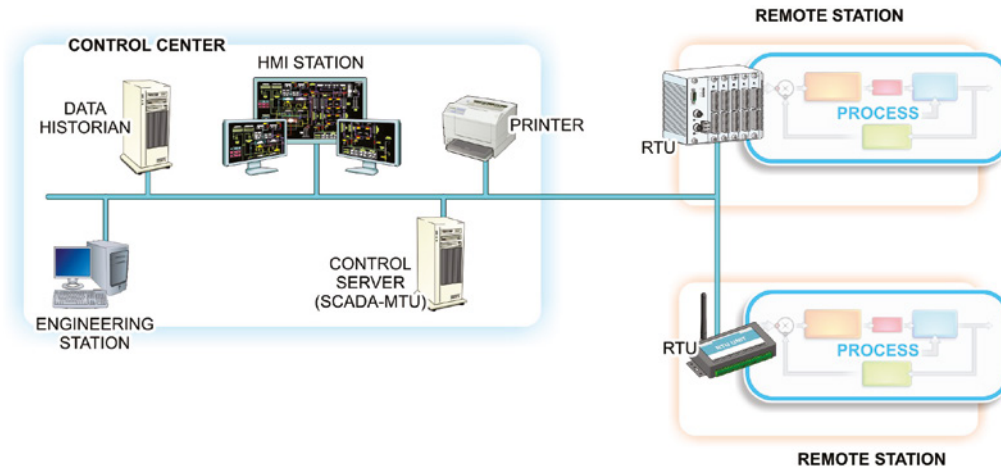
While there have been different current loop standards presented, the 4 to 20 mA DC current standard has been the go-to standard for the industrial sensor market. This standard offers linear signal response, good noise immunity, longer transmission distances, and intrinsic safety for personnel and in hazardous environmental conditions.

RTUs can also provide analog and digital outputs to work with a wide array of different control devices. However, analog outputs are not commonly used with RTUs. The digital outputs provide On/Off control for actuators such as electrical circuits, solenoid valves, lights, and heaters, etc., as needed to manage the process. RTUs that do offer analog output channels can be used to provide continuously variable control of devices such as valve positioners and heating elements.

Unlike PLCs, RTUs are not designed to be stand-alone controllers. Instead, they are better suited for operations in widely distributed control systems. While they have internal memory and do control local activities, they are designed to work with a supervisory controller in distributed or SCADA-based control systems. However, they can also receive process data from local IED controllers.

Communications with supervisory controllers and IED controllers are conducted using standard communication media and protocols. These include RS-232 and RS-485 serial connections as well as Ethernet network connections. Modbus is the prevalent protocol for communicating with RTUs.

Figure 1.10 illustrates a typical RTU implementation. In this example, multiple RTUs are involved in controlling different sections of a distributed process. As with the earlier PLC example, the RTUs maintain local control under the direction of the remote supervisory controller.

FIGURE 1.10 A typical RTU implementation

Intelligent Electronic Devices

In an electric power generation and distribution environment, a third type of intelligent process controller is becoming more popular—the *intelligent electronic device*, or *IED*. These controllers are a form of RTU designed to provide protection, control, monitoring, and communications directly with a supervisory controller. These devices provide a direct interface for monitoring and controlling the different sensors and actuators in the process, and they can communicate directly with the supervisory controller, a local RTU, or other IEDs.

Like RTUs, IEDs typically have small memory units that hold programming for controlling the local process so they can act without direct or constant instructions from the supervisory controller; however, they are not designed to take over full control of a process. Common IED applications include intelligent protective relays, digital fault recorders, power/current/voltage meters, and RTU functions.

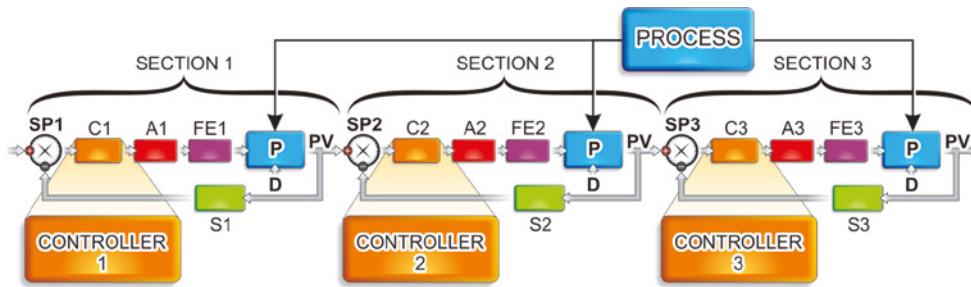
Distributed Control Systems

When processes become too complex for a single controller or its components are geographically separated, it becomes necessary to distribute the control function over multiple controllers to form a *distributed control system (DCS)*.

Figure 1.11 shows a process that is segmented into three discrete subsections, or *process units*, each of which has its own local controller. A unit process is defined as a group of operations within a production system that can be defined and separated from the other unit processes of the system. Each process unit is defined by a specific set of inputs and outputs associated with the tasks the process unit was designed to perform. Even though the

process control function has been distributed across multiple controllers, the control system is not complete. In this example, there are three different devices applying control functions to their segments of a continuous process without regard to activities occurring in the other segments.

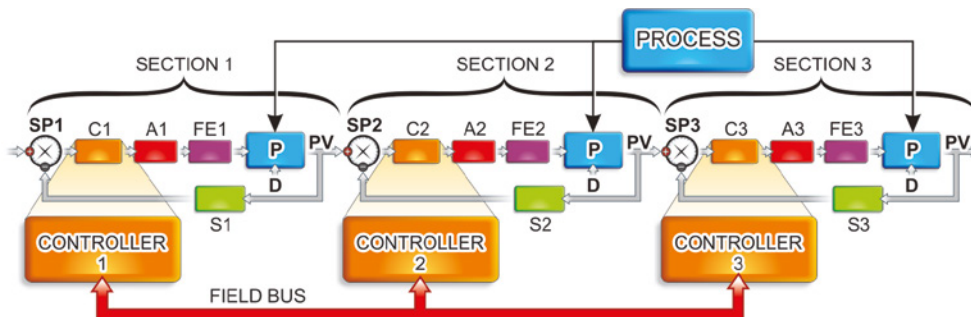
FIGURE 1.11 Distributed controllers



Field Buses

For efficient control of the entire process, some additional control method must be added to the control system to coordinate the activities of the three local controllers. The most fundamental method of doing this is to interconnect the controllers and then make one of them the *master controller*, as illustrated in Figure 1.12. The controllers are physically linked together through a *field bus* and logically linked through an industrial communications protocol. The protocols used over these buses include the Modbus and DNP3 protocols described in detail in the Industrial Network Protocols section of Chapter 2.

FIGURE 1.12 A master controller configuration



A field bus can be any one of several proprietary instrumentation buses designed by industrial control groups to provide communication and coordination between intelligent control devices. These buses can also be used to connect smart IED sensors and actuators to the controllers and eliminate the need to construct *point-to-point wiring* bundles from each process unit's controllers to their sensors and actuators.*

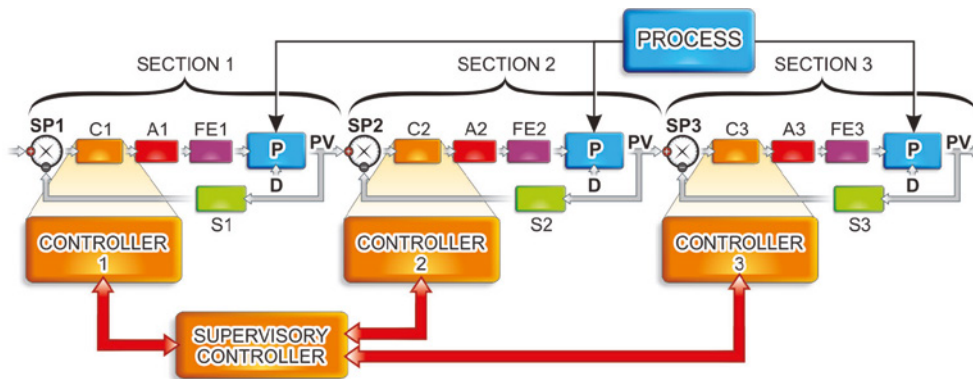


*Smart IED devices can be added to a field bus provided they can communicate through the same protocol as the other devices on the field bus. However, analog and non-microprocessor-based digital sensors and actuators still require independent wire runs between the devices and the controller's inputs and outputs.

Supervisory Controllers

The other method commonly used to efficiently control multiple process units in a distributed process operation is to add a *supervisory controller* to the ICS, as illustrated in Figure 1.13. In this configuration, the supervisory controller is programmed to monitor the operation of each local field control device and send coordinating instructions back to each controller as needed. In such systems, the supervisory controller does not directly control the different process units; it merely oversees and coordinates the operations of their local controllers.

FIGURE 1.13 Adding a supervisory controller



This arrangement represents a typical DCS that would be implemented to efficiently control a complex or widely distributed process. As with the previous example, the controllers in this distributed ICS could be interconnected through any one of several field bus types.

This distributed intelligence model optimizes the computing power of all the control devices to execute, control, manage, and protect the complete process. The local controllers

are typically intelligent devices attached directly to the input and output devices used to monitor and control their portions of the overall process.

Most industrial process control scenarios require high-speed, real-time data acquisition and control functions to maintain proper control of the process. This is a very different requirement than those typically applied to enterprise computing devices that typically do not need to process data in real time.



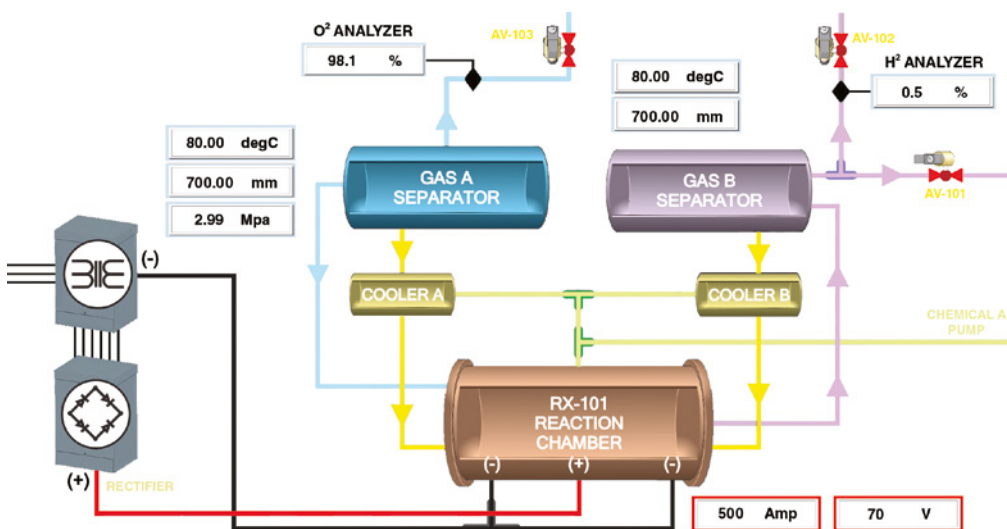
One of the key differences between intelligent devices designed for use in industrial control systems and those designed for enterprise computing and networking environments is the need for real-time processing. This means that ICS devices and programming must be geared to high-speed, low-overhead processing.

Because the supervisory controller is not directly involved in the details of controlling the process, it does not need to be optimized for speed. These controllers are often normal stand-alone computers or industrial servers running supervisory control and data acquisition software applications.

The presence of the local field controllers enables more task-specific intelligent processing to be performed local to the process, while the supervisory controller provides coordination and cooperation between these devices through some type of industry-standard communications channel.

In addition to interfacing with the field-level controllers, the supervisory computers often provide interactive visual control panels, such as the one depicted in Figure 1.14, for human operators involved with the process. This control panel is referred to as a *man-machine interface (MMI)* or a *human-machine interface (HMI)*. The interactive portion of the interface provides human operators with on-screen tools to adjust or override control actions that they see or feel are not occurring as they should.

FIGURE 1.14 Providing the HMI



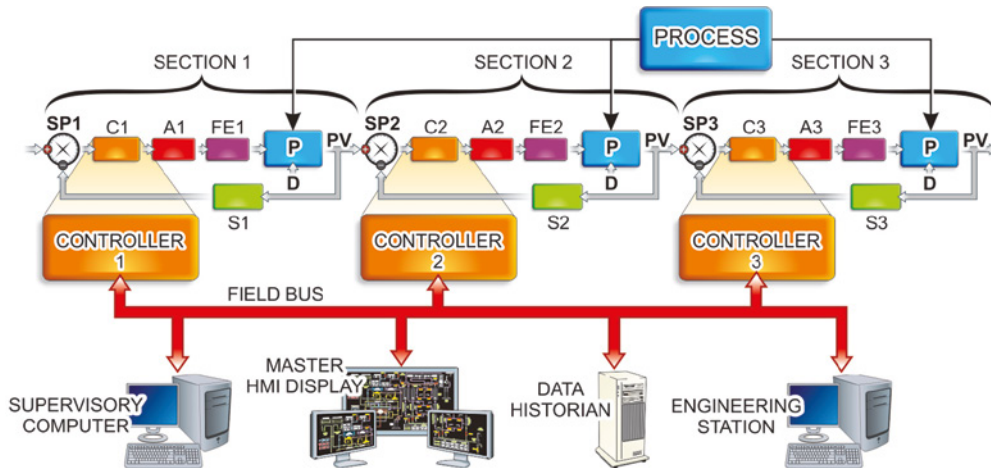
Other ICS Buses

As you saw in previous illustrations, in addition to being connected to the field bus, the controller can also be connected into a local area network that connects it to two standard OT network components.

- *The engineering workstation:* This computing device is used to program the field devices for the current operations.
- *The data historian:* This device contains a database that is used to collect and store process values for inspection and processing.

These units are interconnected to the controller through a separate local area network (LAN) referred to as the *local control loop*. Figure 1.15 depicts a typical ICS with a local control network loop. This type of network loop is typically implemented in the form of a TCP/IP-based Ethernet network segment. In an ICS environment, it has become common to refer to this network segment as the *operational technology (OT)* network to differentiate it from the organization's IT network.

FIGURE 1.15 Adding a supervisory network loop

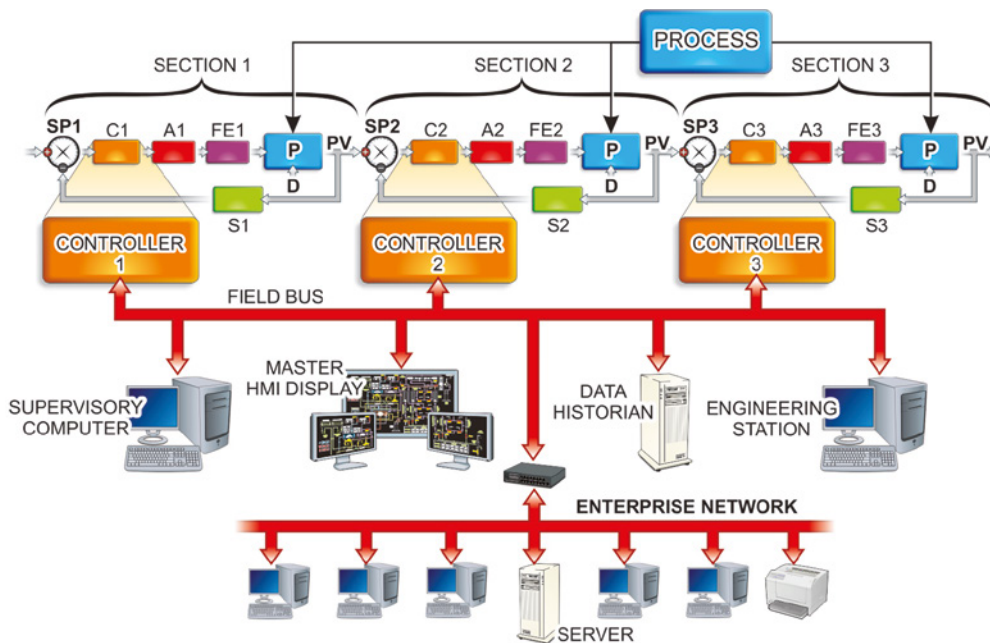


Depending on the complexity of the ICS, the network may be divided into multiple control segments or loops, as illustrated in Figure 1.16. In this example, the complete network structure consists of four distinct network segments and types, shown here:

- *A field bus loop:* This loop provides direct interaction between the local field devices and the sensors and actuators. The field bus is commonly used to connect PLCs to the various input sensors and output actuators. It can also connect to a separate human machine interface console used to display the activities of the process and its various sensors.

- *A local control/supervisory loop:* This loop provides direct interaction between the local field devices and the components of the distributed control system (data historian, engineer's station, HMI, and supervising computers).
- *The organization's local area network:* This loop provides connectivity between the organization's IT network and its ICS network. This connection represents a path outside of the organization's ICS, which opens the network to possible manipulation from non-ICS personnel within the organization.
- *The organization's IT network:* This loop provides connectivity between the organization's local IT network and its wide area network connections. It also provides a pathway between the ICS and a world of possible manipulation by nonorganization personnel.

FIGURE 1.16 Multiple ICS network loops



Network gateway devices are used to translate between different network types, such as a given field bus type and a TCP/IP-based Ethernet network. For example, the connection that brings the field bus and the local control LAN together in the previous example must translate between the physical and logical protocols each segment is based on.

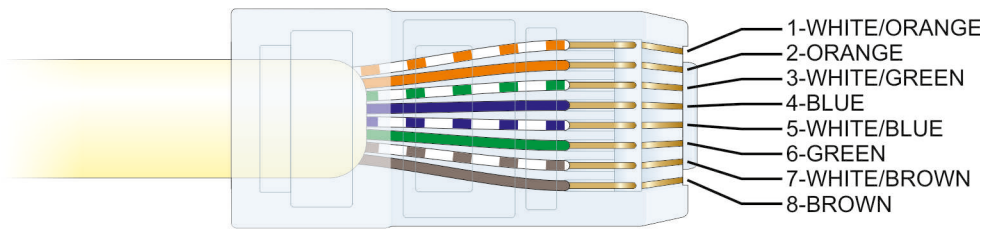
Ethernet I/O Modules

The field bus and local control network portions of the ICS network have historically been implemented over asynchronous serial network topologies, such as standard RS-232 and RS-485 serial bus connections. However, the industrial controls community has slowly come around to the idea of adopting the *Ethernet/IP 802.x suite* of standards for their control and data communications. It has become increasingly popular in industrial control settings.

Ethernet has been the connectivity standard for IT networks since the 1990s. It employs a physical star topology (hub and spokes), even though it actually operates as a logical bus topology. The full suite of Ethernet standards runs across many different media types including twisted-pair copper cabling, fiber-optic cabling, and wireless Wi-Fi channels.

Figure 1.17 shows the physical connectivity of a standard hardwired Ethernet connection. This connection uses twisted-pair copper data cables that are terminated in 8P8C modular plugs and jacks (sometimes incorrectly referred to as RJ-45). In industrial settings, these connections are wired according to TIA/EIA-568-BC standards.

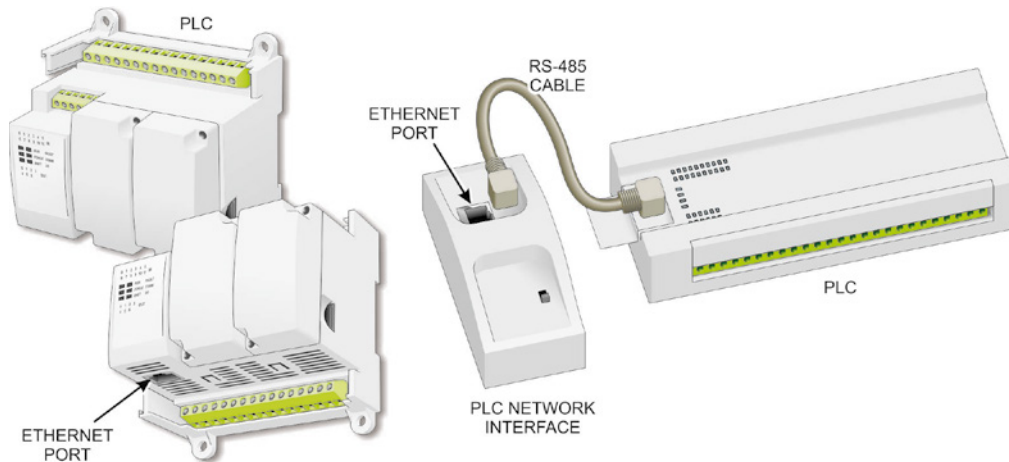
FIGURE 1.17 Ethernet connections



RJ-45 CONNECTOR - T568B STANDARD

The adoption of Ethernet/IP technologies and related techniques has led to a convergence of organizational enterprise networks with their industrial control network counterparts. With both portions of the network integrated into a cohesive data communications vehicle, the organization is enabled to apply real-time production data to its business decisions.

Modules for connecting PLCs to an Ethernet network have historically been separate network interface adapters that involved RS-485 connections between the PLC and the Ethernet adapter and an Ethernet connection with the rest of the network. However, newer PLC models include built-in Ethernet interfaces. Figure 1.18 illustrates the difference in these two approaches.

FIGURE 1.18 PLC Ethernet connections

Supervisory Control and Data Acquisition Systems

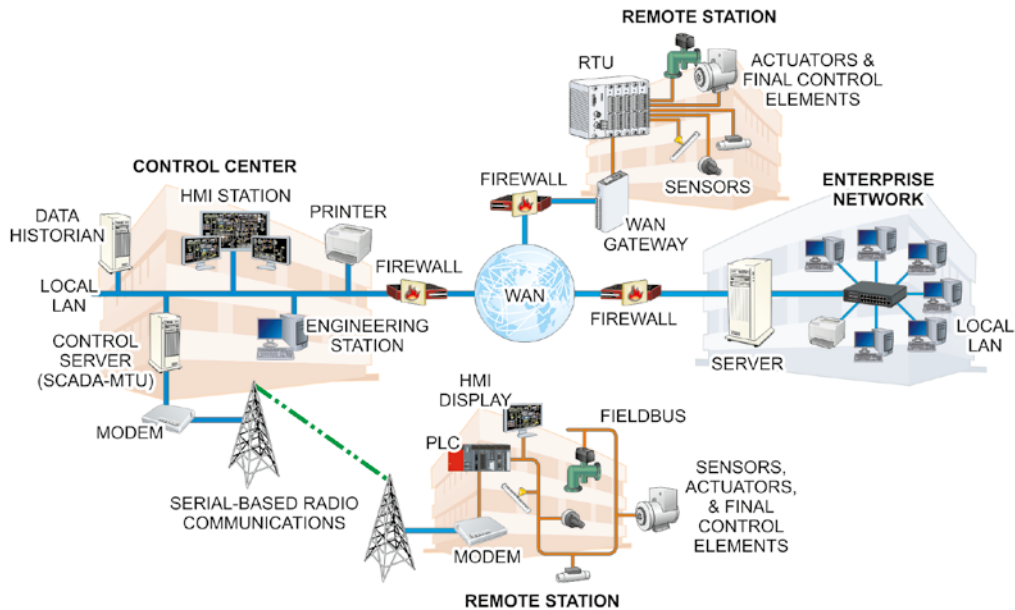
In some processes, such as an oil pipeline control operation, the different control components of the process may be separated by large distances. In such cases the local controllers must be connected to the supervisory controller through long-distance communications technologies such as radios, telephony, satellites, or wide area networking.

As its name implies, a *supervisory control and data acquisition* (SCADA) system is a type of distributed control system that provides two distinct functions: data acquisition (input) and supervisory control functions (output). As you saw earlier in this chapter, PLCs, RTUs, or IEDs typically provide local control of the processes they are monitoring. However, they also package the *acquired data* and transmit it to the supervisory control system over some type of industrial communications link or network connection.

Because industrial processes operate in real time, the operation of the individual local controllers in a distributed control system must be synchronized with each other. The SCADA controller is responsible for providing a common clock signal to coordinate the actions of the different controllers.

The *supervisory control* portion of the SCADA system monitors the data received from its local control devices and stores the information for processing, analysis, and/or response. Responses from the SCADA system are typically reserved for performing supervisory interventions or responding to alarm conditions in the process (such as a motor overheating, a sensor reading out of range, or a cooling system failure). The SCADA system also provides the HMI interface that enables human operators to monitor and assume direct control of the process control system.

Physically, the SCADA system is an industrial software application running on some type of computer platform. These units are referred to as *SCADA servers* or *SCADA masters*. SCADA masters have traditionally communicated with their local control devices using industry-standard ICS protocols and field buses. This arrangement is depicted in Figure 1.19.

FIGURE 1.19 Adding the ICS segment to the network

SCADA servers are also capable of operating within the organization's enterprise network. This is accomplished using standard IT network protocols running over standard IT networking infrastructure.

Part of that software application is a database management system that stores historical data in the form of control points referred to as *tags*. Tags basically consist of two elements: a data point and a timestamp. With these two pieces of information the SCADA system can generate tracking and trending data for graphical display or auditing purposes. This database is called the *historian*.

The SCADA software provides the supervisory role for all the PLCs operating in the process. It also provides the HMI that enables human operators to observe the operating parameters of the different processes and take charge of the processes to change parameters or make corrections.

Over time, SCADA systems have migrated from large mainframes (first generation) at the organization's offices, to individual task computers networked together through LANs (second generation), to networked wide area SCADA systems (third generation), and now to cloud-based, Industrial Internet of Things (IIoT) SCADA systems (fourth and current generation).

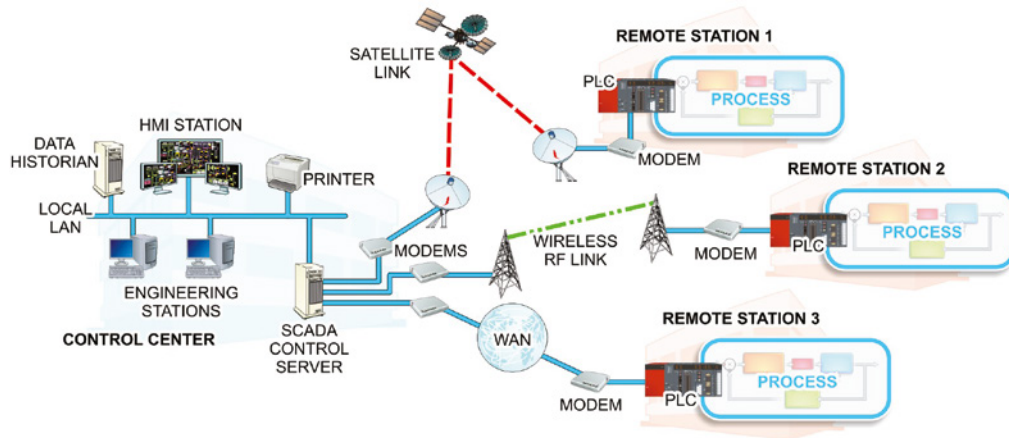
System Telemetry

As mentioned earlier, *telemetry* is the process of using sensors to collect information in a remote location and transmitting it to another location for processing. This is a prerequisite for widely distributed control systems. There are many industries (airlines, water, gas, oil,

and electrical transportation and distribution) that require operations in geographically separated locations to be coordinated through widely distributed control systems.

Figure 1.20 illustrates a widely distributed control system where controllers in three remote field sites are monitoring and controlling three different portions of a distribution process. Using modern data communication links, these controllers can be physically located away from the process area in isolated environments.

FIGURE 1.20 ICS telemetry systems

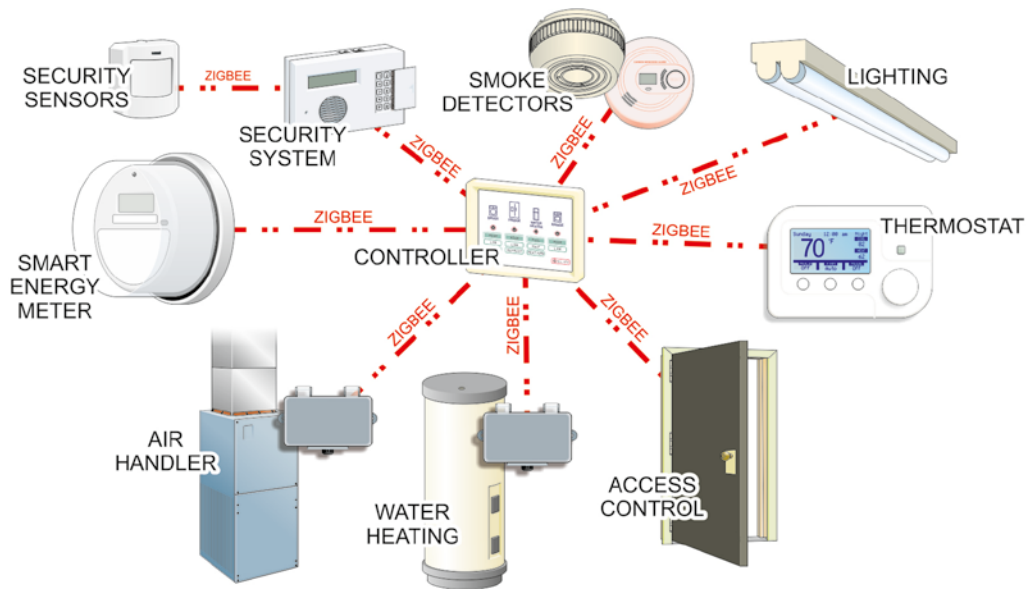
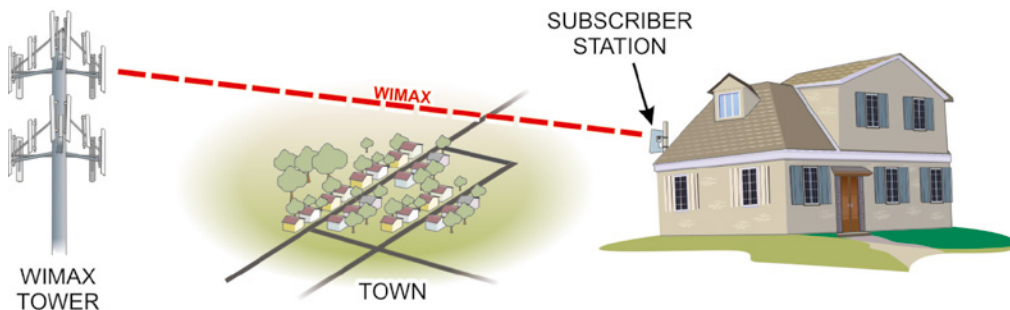


In this example, the remotely located SCADA controller is connected to each field site using a different long-distance communication link. Station 1 connects to the Control Center through a wireless RF communication link, while Station 2 employs a satellite link and Station 3 uses a wide area network (WAN) connection.

Industrial and utility networks also employ different wireless communication protocols to transmit data and telemetry throughout their processes. In particular, the WiMax and Zigbee wireless protocols have made significant inroads into industrial control networks, particularly in electrical utility network settings.

The *Zigbee* (IEEE 802.15.4) standard is a wireless, mesh-networked personal area network (PAN) protocol that provides for a 10-meter communication range with data transfer rates at 250 Kbps, as shown in Figure 1.21. The Zigbee standard has been embraced by the smart home automation and industrial controls communities, as well as several areas of the smart grid consortium.

The IEEE 802.16 – WiMAX specification was established to provide guidelines for wider area wireless networking capabilities. WiMAX is a broadband wireless access standard designed to provide Internet access across large geographic areas, such as cities, counties, and in some cases countries, as shown in Figure 1.22. It is also designed to provide interoperability with the 802.11x Wi-Fi standard.

FIGURE 1.21 Zigbee PAN**FIGURE 1.22** A WiMAX network

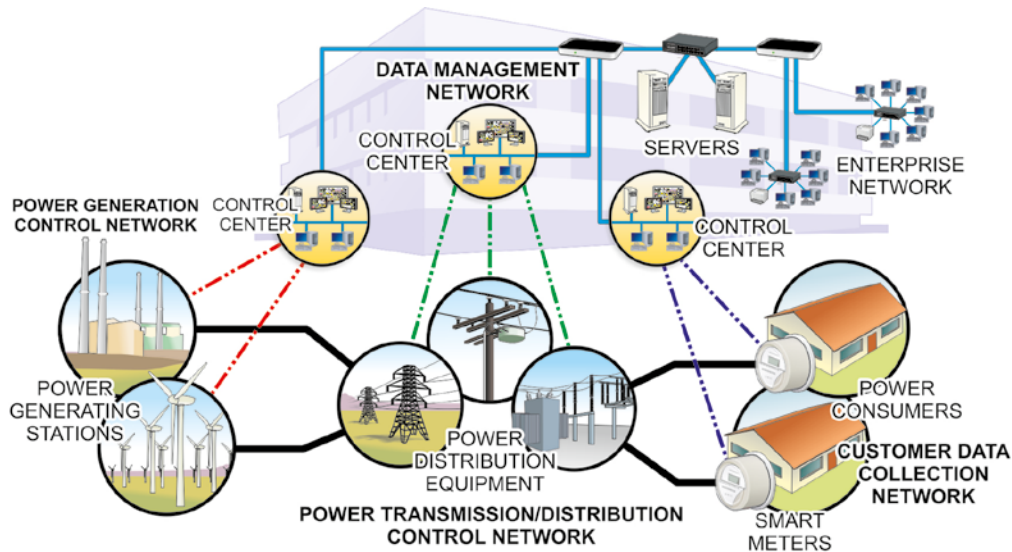
Utility Networks

Virtually all utility organizations rely on *wide area networks* to optimize the efficiency of their operations. This is illustrated in Figure 1.23, which depicts a typical electrical utility's *smart grid* network infrastructure that spreads across four different network types—two wide area networks and two local area networks:

- The power generation control network (a dedicated industrial control network)
- The power transmission/distribution control network (a widely distributed industrial control network)

- The customer (meter) data collection network (a wide area network)
- The host utility's data management network (part of the in-house enterprise network)

FIGURE 1.23 A utility network system



One of the most important aspects of telemetry is *metering*. A metering device, or meter, is an endpoint sensor that measures and records the quantity of a substance (collects data). The primary function of any utility meter is to measure customer usage—electricity, water, gas, oil, etc.

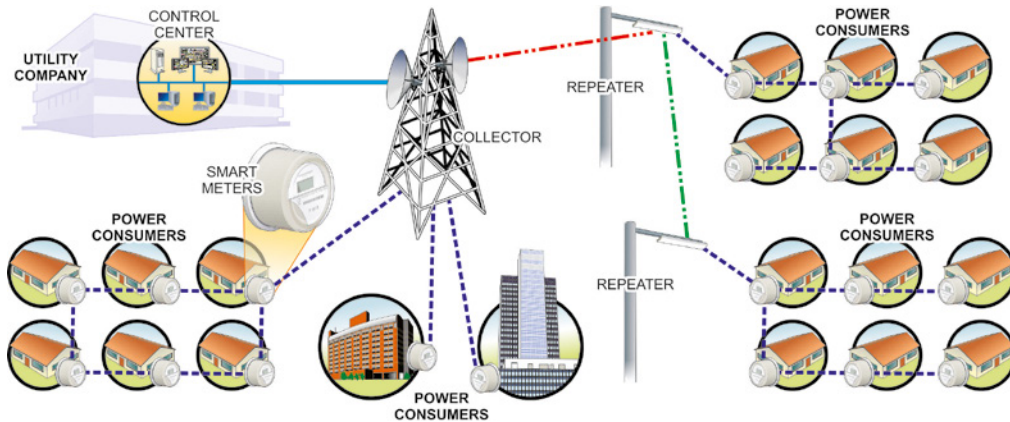
The utility's customer (meter) data collection system collects usage information about every customer connected to its transmission and distribution system through the smart meters mentioned earlier. These metering network devices are typically configured to do the following:

- Communicate with the other smart grid components in the user's *home area network (HAN)*
- Provide current cost information to the members of the HAN
- Provide current *time-of-use (TOU)* information to the members of the HAN
- Communicate with the host utility across the WAN
- Package customer data for transmission to the host utility
- Interact with the host utility's *meter data management (MDM)* system

Figure 1.24 shows a typical *advanced metering infrastructure (AMI)* wireless mesh network architecture used to provide communications throughout the metering network. These

networks are designed to provide reliability, redundancy, and bandwidth while still meeting the budgetary requirements of the electrical utility. In addition, they must enable several different types of devices to communicate with each other.

FIGURE 1.24 AMI mesh architecture

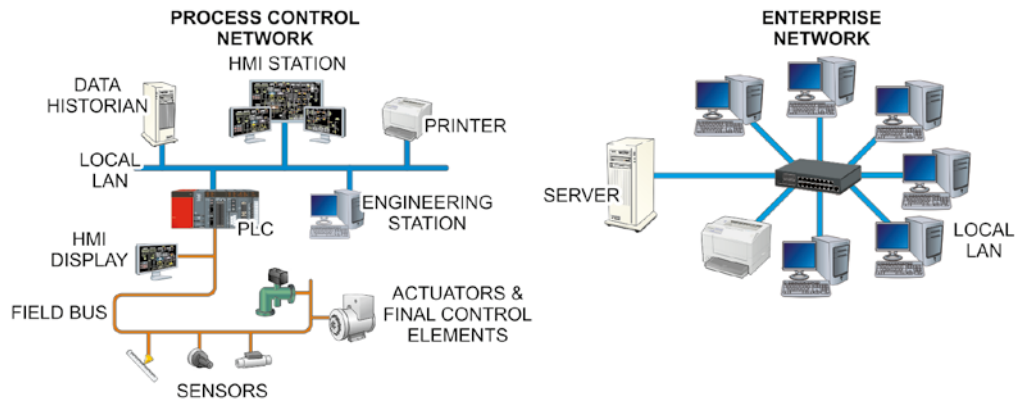


This example depicts three distinct zones networked together through two aggregators and a collector. In residential areas, the smart meters are connected in neighborhood area network (NAN) meshes and communicate with each other (meter-to-meter) and with aggregators (meter-to-aggregators) as well as directly with the collector (meter-to-collector).

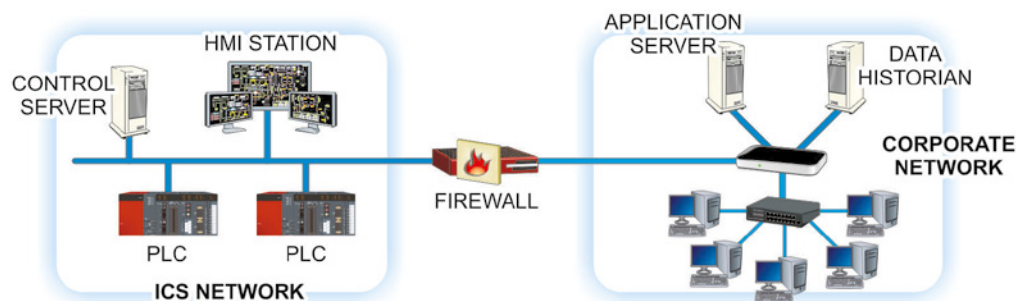
The aggregators communicate directly with the collector (aggregator-to-collector). Notice also that industrial and larger commercial customers connect directly to the collector. The collector is responsible for communicating with all the meshes to handle all the functions listed earlier in this section. In addition, it must have the communication and computing capacity to do this for thousands or tens of thousands of meters. Security issues associated with these networks and their devices are presented in Chapter 4, “ICS Module and Element Hardening.”

OT/IT Network Integration

Historically, industrial production organizations have operated their networks as two separate entities: the enterprise (IT) network and the process control (OT) network, as illustrated in Figure 1.25. The IT network is designed to process and store business data, while the OT network is designed to control processes that produce products and generate revenue. Normally, great effort is applied to minimizing the interactivity points between these two networks.

FIGURE 1.25 Industrial networks

However, in many organizations, the supervisory controller has been added to their existing enterprise network structure as a separate network segment, as illustrated in Figure 1.26. This connection permits other business operations to interface with the production sector of the company. However, it also creates an access path between the two networks that exposes the ICS to new threats typically associated with IT networks. As you will see in greater detail in Chapter 3, “Secure ICS Architecture,” the industrial control portion of such a network should be segregated or heavily segmented from the organization’s enterprise network.

FIGURE 1.26 Adding the ICS segment to the IT network

Because the movement to connect OT and IT networks together has grown to a significant level, the *International Society of Automation (ISA)* has developed a set of standards known as *ISA-95* to define automated information exchange interfacing between enterprise and industrial control system networks.

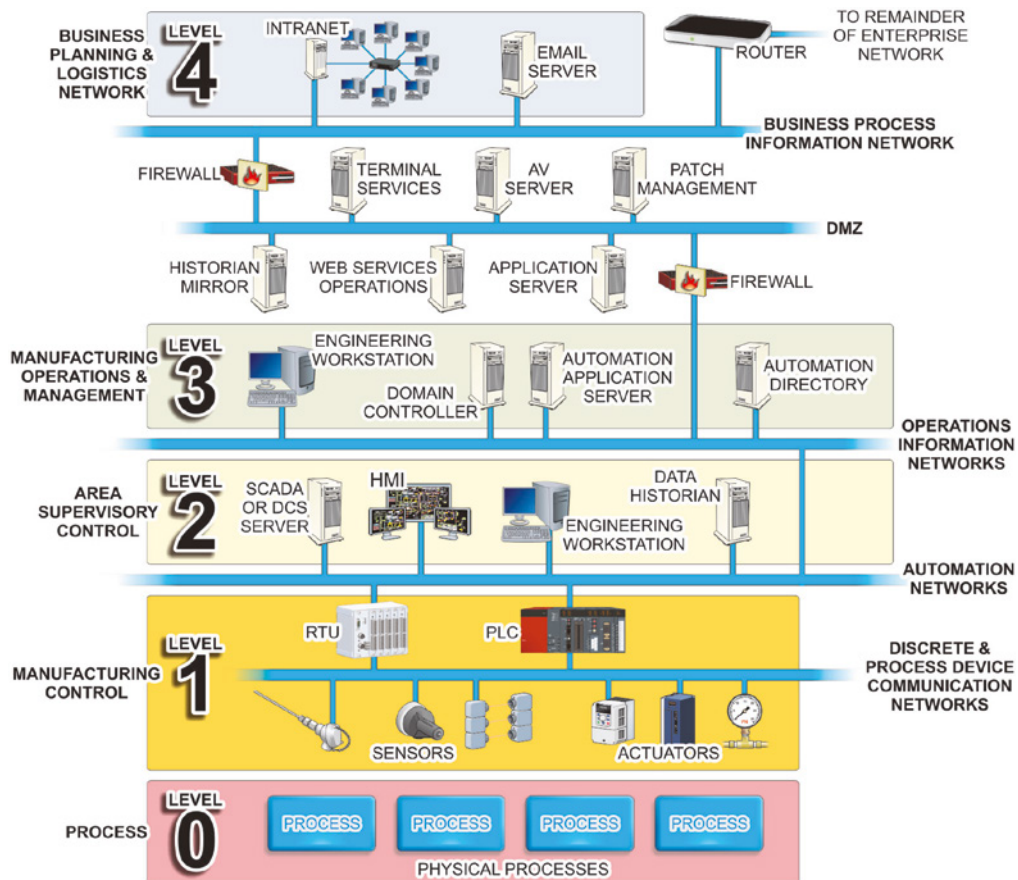
The original version of this standard was referred to as the *Perdue Enterprise Reference Architecture for ICS cybersecurity* and is used for grouping IT/OT network segments into security zones. This set of standards establishes a five-level integration process:

- Level 0: Physical Protection
- Level 1: Production Process Sensing and Manipulation

- Level 2: Automated Control of the Production Process
- Level 3: Workflow Control
- Level 4: Basic Plant Scheduling

Levels 0, 1, and 2 apply to the ICS functions of the organization provided by the SCADA or DCS systems, while level 4 maps in the business functions of the organization that track to the enterprise network's operation. Level 3 functions provide the information exchange interface between the OT and IT networks. Figure 1.27 illustrates the distribution of the different network devices described in the ISA-95 standard.

FIGURE 1.27 The ISA-95 standard



While the ISA-95 architecture model remains the standard for IT/OT integration, advances in IIoT and cloud technologies are beginning to redefine manufacturing integration. The question going forward is whether the ISA-95 model will be taken over by a radically different model or whether these new technologies (IIoT, cloud computing, and edge

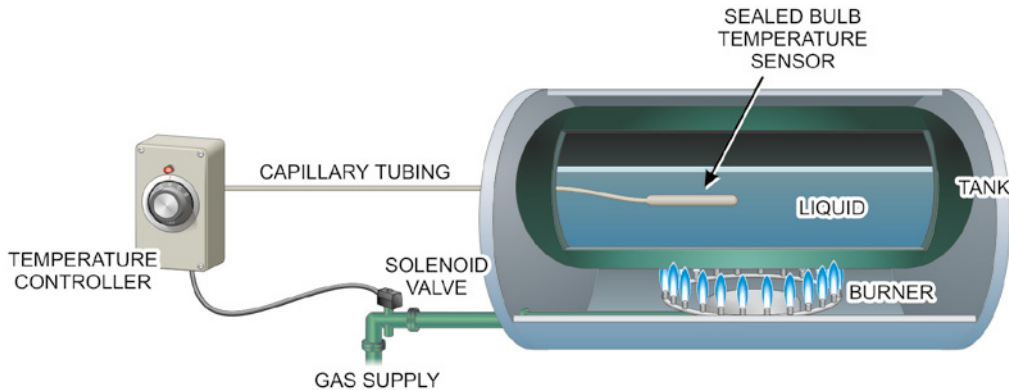
computing) will converge with the basic structure of the ISA-95 model. Currently, members of the ISA-95 committee are working on additions to the standard to accommodate such new industry requirements as IIoT and Industry 4.0 standards and practices.

Industrial Safety and Protection Systems

Industrial production and utility environments tend to be inherently more hazardous than enterprise network environments. Basically, if a word processor crashes or is compromised, the user might be upset and likely have to do a lot more typing to recover their lost information. However, if an industrial control process is compromised, the organization could suffer loss of productivity, profitability, equipment, a portion of the community, or worse.

As an example, re-examine the simple liquid heating process described in Figure 1.2 and represented in Figure 1.28. While this process already has a *process control system* in place to control the temperature of the fluid in the tank, there are several potentially hazardous conditions that could occur if any part of that system malfunctioned or failed. As such, these hazards become part of the risk analysis process that makes it different than a risk assessment performed for an enterprise environment.

FIGURE 1.28 A simple heating process revisited



A quick examination of the process shows several potential hazards:

- The tank is heated with a gas-fed heating system.
- The tank contains a liquid that is being heated.
- The temperature sensor, controller, and solenoid valve all represent single points of failure.

The process control system depicted offers no provisions for monitoring or controlling the gas other than the single solenoid valve. As such, the gas heating system represents a number of potentially explosive conditions, as any leak in the system provides an opportunity for uncontrolled ignition.

For example, if the gas piping *outside the tank* developed a leak, the gas would exit the pipe and fill the space around the leak. If an ignition source is introduced within the area where the gas is accumulating, an explosion will occur. In addition, the unignited gas could become a hazard to humans working in the area as it mixes with the air they are breathing.

There is also no provision for monitoring the condition of the gas within the tank. If the fire at the burner went out, this system would still provide gas to the burner. This would allow the gas to build up inside the tank, posing possible uncontrolled combustion hazards if the burner is reignited or personnel open the tank to examine the burner system.

The liquid being heated inside the tank may also be a source of uncontrolled explosion. As the liquid is heated, its molecules gain energy, move more rapidly, and move farther apart (the liquid expands). At some point, it will change from a liquid state to a gaseous state. When this occurs, the pressure inside the tank increases. If left unvented, the pressure can eventually increase to the point that the tank ruptures—maybe violently. The process control system depicted has no provision for monitoring the amount or condition of the liquid inside the tank.

The fact that many of the process control system's devices are the only devices performing a given function makes them all potential sources of problems. For example, if the temperature sensor fails for any reason, the controller will not receive the feedback signal it needs to control the process properly. If the sensor fails so that the controller thinks the temperature is lower than its set point, it will continue to apply gas to the burner, causing the same hazard conditions described earlier.

If the controller fails, the actuator will not receive the error correction signal it requires to control the gas flow and heating process. Depending on the nature of the failure and the design of the final control element, the tank could be allowed to overheat and produce the potential explosion hazards described earlier. Ideally the design of the system is such that any failure would cause the final control element to *fail safe* (shut down the gas flow to the burner).

As you can see, even simple processes like the one presented here provide multiple potential threats to equipment, personnel, and productivity. As such, industrial safety systems must be added to the basic process control system to mitigate the risks pointed out by these concerns. This concept is discussed in detail in Chapter 10, “ICS Security Monitoring and Incident Response.” The remainder of this chapter will be used to introduce safety instrument systems and discuss common safety and protection subsystems.

Safety Instrument Systems

Safety instrument systems (SISs) are basically automated process control systems specifically designed to monitor and control conditions in and around the process that have been defined as unsafe or potentially unsafe. The SIS is typically created as an integral part of the overall ICS package (but not the same components). The SIS must be able to successfully perform its functions when the process control system fails. Together these two systems are referred to as the *integrated control and safety system (ICSS)*.

Like the ICS, the SIS is composed of sensors, controllers, and actuators. What the SIS does and to what level is determined through a formal *hazard and operability (HAZOP)* study performed as part of the *process hazard analysis (PHA)* process required for every industrial process. This process is used to identify hazardous scenarios that require *safety instrumented functions (SIFs)* to mitigate. The IEC 61508, 61511, and ANSI/ISA 84 standards define a SIF as “a safety function with a specific *Safety Integrity Level (SIL)* which is necessary to achieve functional safety.” This process will also be discussed in detail in Chapter 10.



The standards all address establishing specific requirements for SIS systems:

- IEC 61508, “Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems (E/E/PE, or E/E/PES)”; IEC 61511, “Functional safety – safety instrumented systems for the process industry sector”; IEC 61513 (nuclear); IEC 62016 (manufacturing/machineries)
- ANSI/ISA 84, “The Standard for Safety Instrumented Systems”

The various SIFs identified by the HAZOP are brought together to design and implement the complete SIS. The SIL for each SIF can be defined either as the amount of defined risk reduction to be provided by the safety instrumented function or as the level of dependability of the SIF. There are four discrete SIL ratings being used:

- *SIL 1*: The lowest associated safety level/highest probability that a system will fail to perform properly.
- *SIL 2*: Increased associated safety level/decreased probability of failure to perform properly. These systems are generally more complex than SIL 1–rated systems and tend to be more expensive to install and maintain.
- *SIL 3*: Highest usable rating for associated safety level/decreased probability of failure to perform properly. Because systems rated at this level tend to be expensive to acquire and maintain, many organizations will reengineer their processes to work with lower-rated systems when the results of a HAZOP specify this level of SIL.
- *SIL 4*: The highest associated safety level/lowest probability that a system will fail to perform properly. However, these systems are too complex and costly for most process industries to install and implement. Any process that requires an SIL 4 system should be considered as having fundamental design problems and be redesigned.

SIS Equipment

The safety sensors are designed to monitor different areas of the production environment to detect those conditions that have been defined as unsafe or hazardous through the risk assessment process.

The safety controller is responsible for acquiring the sensor’s information and acting on it based on its design and programming. The safety controller may be programmed to provide

several different responses, depending on the nature of the hazard detected and the level of protection deemed necessary to mitigate the safety condition:

- *Unit safety shutdown (USD)*: A USD is a shutdown of an individual process or utility system to prevent equipment from operating in an unsafe manner (outside of process limits). At this level, the safety control system shuts down the local process where the safety condition has been detected. However, it will not affect the operation of other processes running in the plant.
- *Process shutdown (PSD)*: This type of shutdown results from undesirable process conditions that may degrade the quality of the product if allowed to continue. This level of shutdown may shut down and isolate related processes or equipment to prevent the condition from affecting those processes, leading to an emergency shutdown condition.
- *Emergency shutdown (ESD)*: An ESD results from a more serious condition detected in the process that threatens the process equipment, personnel, environment, plant, or community. This type of shutdown typically results from conditions related to serious safety concerns, such as runaway process variables.
- *Emergency depressurization shutdown (EDP)*: This level of shutdown is actually an extension of an ESD in that shutdown of the process and its related equipment and processes may cause some undesirable conditions to exist due to the ESD (such as pressure built up in gas lines or inside vessels like the tank in Figure 1.28).

The SIS also employs actuators that operate to control or remove the unsafe conditions. These actuators must be designed and selected to perform specific actions that will limit or remove the threats caused by the unsafe condition(s). SIS system components and operations are designed and selected with special attention to their failure states (what they do or how they respond when something fails). There are two basic modes to consider:

- *Fail safe* is a device or system designed so that in the event of a power or component failure, the process being controlled will remain in its safe condition (on or off). For example, the gas control valve in the sample process should be selected so that it naturally fails safe (moves to a closed position) any time it loses signal from the controller. This would ensure that the gas flow into the tank would be cut off in the event of any failure.
- *Fail secure* is a device or system designed so that the process being controlled will assume its most secure condition in the event of a power or component failure.

Because the security controller is primarily a security device, one of its main responsibilities is to provide proper notification when a security event occurs. When the controller receives an active input signal from one of its security sensors, it evaluates the conditions presented according to its programming (and the type of emergency response required) and, if necessary, sends the appropriate alarm signals to annunciators (sirens or bells). It may also activate any number of visual indicators such as flashing lights, operator panel lights, or icons on a control panel.

The controller may also communicate with designated security and supervisory contacts (security supervisors, monitoring services, or emergency services) as directed by its programming. These systems are designed to react when no one is present. They may use any of several methods to accomplish this:

- *Dial-up telephone connections:* Use a telephone dialer to alert remote security contacts that a hazardous condition exists over a standard telephone line.
- *Cellular Channels:* Use a cellular channel to send prepared text messaging to designated security or supervisory contacts.
- *IP-based notification:* Use an IP network (such as the Internet) to notify designated security and supervisory personnel concerning a hazard condition.

Redundant Systems

Component and system *redundancy* is one of the most basic practices in industrial security. We've already identified several key components that represent *single points of failure* in the simple process example presented in this chapter. The reason the SIS is made up of different components than the process control system is that the SIS must step in and take control when a component in the process control system fails. If they are the same device in both systems, then both systems fail.

For example, to address the hazards associated with the process that were identified earlier in the chapter, we could look at adding several sensors to the system:

- Gas detection sensor outside the tank
- Flame detection sensor inside the tank
- Pressure sensor inside the tank
- Safety temperature sensor inside the tank

In each case, these sensors are redundant to the process control sensors in the original design.

Basic actuators that can be added to the process to mitigate potential hazards include the following:

- Manual shut-off valve upstream from the solenoid control valve
- Security shut-off valve between the manual and process control valves
- Pressure relief valve on the shell of the tank

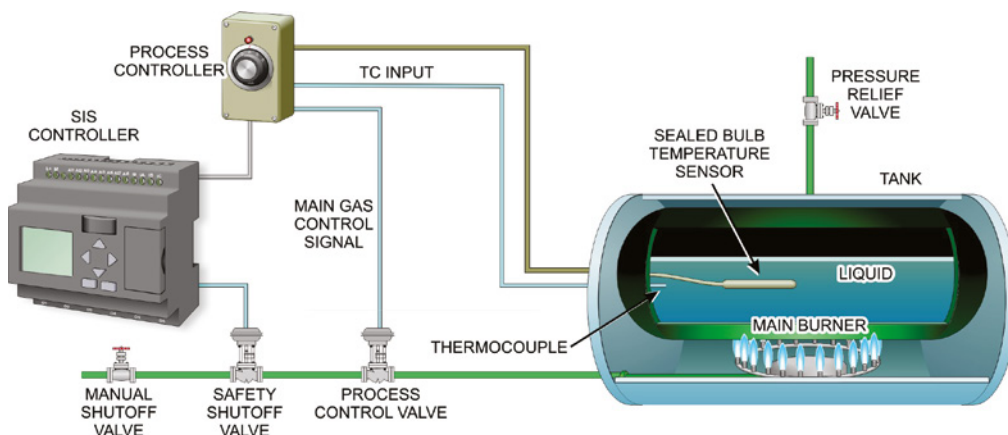
As with the proposed security sensors, these additional actuators are redundant to the actuators in the original process control system design.

Emergency Shutdown Systems

Emergency shutdown systems (EMSS) are a specific type of SIS designed to minimize the consequences of certain emergency conditions. They operate at the prevention safety layer and act to prevent a hazardous event such as a fire, a chemical release, or an explosion from occurring. As systems, they consist of ESD sensors, ESD controller, and ESD actuators.

Returning to our process control example, we can build a simple block diagram of an ESD that could be implemented to perform the shutdown procedure. The foremost consideration for any emergency would be shutting the gas supply off. The redundancy list presented earlier provides two options for doing this—an automated solenoid valve connected to the SIS controller and a manual shutoff valve, as illustrated in Figure 1.29.

FIGURE 1.29 Adding an ESD system



The other hazard mentioned in our quick analysis was that the pressure in the tank could increase to a dangerous level if the burner is allowed to continuously heat the liquid. This would eventually cause the tank to fail in an explosive manner. To mitigate this possibility, a pressure relief valve could be installed on the shell of the tank. When the controller detects a failure, it will cause the valve to fail open, relieving the pressure inside the tank by venting it into the outside atmosphere.

Figure 1.29 also shows the addition of redundant sensors and controller to the original process control system. These devices represent a few of the typical safety sensors found in industrial process Safety Instrumentation Systems. The following sections of the chapter deal with specific safety systems identified in the GICSP certification objectives.

Fire and Gas Systems

Fire and gas systems (FGSs) are part of the SIS that operate at the mitigation safety layer and act to limit the consequences of an ESD event. They are implemented in the SIS to continuously monitor plant activity and in case of hazardous conditions initiate appropriate actions. For example, if an FGS detects a combustible gas (such as the gas being used to heat the tank in Figure 1.29), a toxic gas, smoke, flame, or excessive heat, it may issue a visual and audible warning along with activating a fire suppression system and/or process shutdown.

In our simple process, the FGS would use gas leak detection devices located at intervals and joints along the length of the supply pipe. The controller may be as simple as a PLC