CHAPTER

About Industrial Networks

2

INFORMATION IN THIS CHAPTER

- The Use of Terminology Within This Book
- Common Industrial Security Recommendations
- Advanced Industrial Security Recommendations
- Common Misperceptions About Industrial Network Security

It is important to understand some of the terms used when discussing industrial networking and industrial control systems, as well as the basics of how industrial networks are architected and how they operate before attempting to secure an industrial network and its interconnected systems. It is also important to understand some of the common security recommendations deployed in business networks, and why they may or may not be truly suitable for effective industrial network cyber security.

What is an industrial network? Because of a rapidly evolving socio-political landscape, the terminology of industrial networking has become blurred. Terms such as "critical infrastructure," "APT," "SCADA," and "Smart Grid" are used freely and often incorrectly. It can be confusing to discuss them in general terms not only because of the diversity of the industrial networks themselves, but also the markets they serve. Many regulatory agencies and commissions have also been formed to help secure different industrial networks for different industry sectors—each introducing their own specific nomenclatures and terminology.

This chapter will attempt to provide a baseline for industrial network cyber security, introducing the reader to some of the common terminology, issues, and security recommendations that will be discussed throughout the remainder of this book.

THE USE OF TERMINOLOGY WITHIN THIS BOOK

The authors have witnessed many discussions on industrial cyber security fall apart due to disagreements over terminology. There is a good deal of terminology specific to both cyber security and to industrial control systems that will be used throughout this book. Some readers may be cyber security experts who are unfamiliar with industrial control systems, while others may be industrial system professionals who are unfamiliar with cyber security. For this reason, a conscientious effort has been made by the authors to convey the basics of both disciplines, and to accommodate both types of readers.

Some of the terms that will be used extensively include the following:

- Assets (including whether they are physical or logical assets, and if they are classified as cyber assets, critical assets, and critical cyber assets)
- Enclaves, Zones, and Conduits
- Enterprise or Business Networks
- Industrial Control Systems: DCS, PCS, SIS, SCADA
- Industrial Networks
- Industrial Protocols
- Network Perimeter or Electronic Security Perimeter (ESP)
- Critical Infrastructure.

Some cyber security terms that will be addressed include the following:

- Attacks
- Breaches
- Incidents and Exploits
- Vulnerabilities
- Risk
- Security Measures, Security Controls, or Countermeasures.

These will be given some cursory attention here, as a foundation for the following chapters. There are many more specialized terms that will be used, and so an extensive glossary has been provided at the back of this book. The first time a term is used, it will be printed in bold to indicate that it is available in the glossary.

NOTE

The book title "Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems" was chosen because this text discusses all of these terms to some extent. "Industrial cyber security" is a topic relevant to many industries, each of which differ significantly in terms of design, architecture, and operation. An effective discussion of cyber security must acknowledge these differences; however, it is impossible to cover every nuance of DCS, SCADA, Smart Grids, critical manufacturing, and so on. This book will focus on the commonalities among these industries, providing a basic understanding of industrial automation, and the constituent systems, subsystems, and devices that are used. Every effort will also be made to refer to all industrial automation and control systems (DCS, PCS, SCADA, etc.) as simply industrial control systems or just ICS. It is also important to understand that industrial networks are one link in a much larger chain comprising fieldbus networks, process control networks, supervisory networks, business networks, remote access networks, and any number of specialized applications, services and communications infrastructures that may all be interconnected and therefore must be assessed and secured within the context of cyber security. A Smart Grid, a petroleum refinery, and a city skyscraper may all utilize ICS, yet each represents unique variations in terms of size, complexity, and risk. All are built using the same technologies and principles making the cyber security concerns of each similar and the fundamentals of industrial cyber security equally applicable.

NOTE

This book does not go into extensive detail on the architecture of Smart Grids due to the complexity of these systems. Please consult the book "Applied Cyber Security and the Smart Grid"[1] if more detail on Smart Grid architecture and its associated cyber security is desired.

ATTACKS, BREACHES, AND INCIDENTS: MALWARE, EXPLOITS, AND APTs

The reason that you are reading a book titled "Industrial Network Security" is likely because you are interested in, if not concerned about, unauthorized access to and potentially hazardous or mischievous usage of equipment connected to an industrial network. This could be a deliberate action by an individual or organization, a government-backed act of cyber war, the side effect of a computer virus that just happened to spread from a business network to an ICS server, the unintended consequence of a faulty network card or—for all we know—the result of some astrological alignment of the sun, planets, and stars (aka "solar flares"). While there are subtle differences in the terms "incident" and "attack"—mostly to do with intent, motivation, and attribution—this book does not intend to dwell on these subtleties. The focus in this book is how an attack (or breach, or exploit, or incident) might occur, and subsequently how to best protect the industrial network and the connected ICS components against undesirable consequences that result from this action. Did the action result in some outcome—operational, health, safety or environment—that must be reported to a federal agency according to some regulatory legislation? Did it originate from another country? Was it a simple virus or a persistent rootkit? Could it be achieved with free tools available on the Internet, or did it require the resources of a state-backed cyber espionage group? Do such groups even exist? The authors of this book think that these are all great questions, but ones best served by some other book. These terms may therefore be used rather interchangeably herein.

ASSETS, CRITICAL ASSETS, CYBER ASSETS, AND CRITICAL CYBER ASSETS

An asset is simply a term for a component that is used within an industrial control system. Assets are often "physical," such as a workstation, server, network switch, or PLC. Physical assets also include the large quantity of sensors and actuators used to control an industrial process or plant. There are also "logical" assets that represent what is contained within the physical asset, such as a process graphic, a database, a logic program, a firewall rule set, or firmware. When you think about it, cyber security is usually focused on the protection of "logical" assets and not the "physical" assets that contain them. Physical security is that which tends to focus more on the protection of a physical asset. Security from a general point-of-view can therefore effectively protect a "logical" asset, a "physical" asset, or both. This will become more obvious as we develop the concept of security controls or countermeasures later in this book.

The Critical Infrastructure Protection (CIP) standard by the North American Electric Reliability Corporation (NERC) through version 4 has defined a "critical cyber asset" or "CCA" as any device that uses a routable protocol to communicate outside the electronic security perimeter (ESP), uses a routable protocol within a control center, or is dial-up accessible.[2] This changed in version 5 of the standard by shifting from an individual asset approach, to one that addresses groupings of CCAs called bulk electric system (BES) cyber "systems."[3] This approach represents a fundamental shift from addressing security at the component or asset level, to a more holistic or system-based one.

A broad and more generic definition of "asset" is used in this book, where any component—physical or logical; critical or otherwise—is simply referred to as an "asset." This is because most ICS components today, even those designed for extremely basic functionality, are likely to contain a commercial microprocessor with both embedded and user-programmable code that most likely contains some inherent communication capability. History has proven that even single-purpose, fixed-function devices can be the targets, or even the source of a cyber-attack, by specifically exploiting weaknesses in a single component within the device (See Chapter 3, "Industrial Cyber Security History and Trends"). Many devices ranging from ICS servers to PLCs to motor drives have been impacted in complex cyber-attacks—as was the case during the 2010 outbreak of **Stuxnet** (see "Examples of Advanced Industrial Cyber Threats" in Chapter 7, "Hacking Industrial Control Systems"). Regardless of whether a device is classified as an "asset" for regulatory purposes or not, they will all be considered accordingly in the context of cyber security.

SECURITY CONTROLS AND SECURITY COUNTERMEASURES

The term "security controls" and "security countermeasures" are often used, especially when discussing compliance controls, guidelines, or recommendations. They simply refer to a method of enforcing cyber security—either through the use of a specific product or technology, a security plan or policy, or other mechanism for establishing and enforcing cyber security—in order to reduce risk.

FIREWALLS AND INTRUSION PREVENTION SYSTEMS

While there are many other security products available—some of which are highly relevant to industrial networks—none have been so broadly used to describe products with such highly differing sets of capabilities. The most basic "firewall" must be able to filter network traffic in at least one direction, based on at least one criterion, such as IP address or communication service port. A firewall may or may not also be able to track the "state" of a particular communication session, understanding what is a new "request" versus what is a "response" to a prior request.

A "deep packet inspection" (DPI) system is a device that can decode network traffic and look at the contents or payload of that traffic. Deep packet inspection is typically used by intrusion detection systems (IDS), intrusion prevention systems (IPS), advanced firewalls and many other specialized cyber security products to detect signs of attack. Intrusion *Detection* Systems can detect and alert, but do not block or reject bad traffic. Intrusion *Prevention* Systems can block traffic. Industrial networks support high availability making most general IPS appliances less common on critical networks; IPS is more often applied at upper-level networks where high availability (typically >99.99%) is not such a high priority. The result is that good advice can lead to inadequate results, simply through the use of overused terms when making recommendations.

NOTE

Most modern intrusion prevention systems can be used as intrusion detection systems by configuring the IPS to alert on threat detection, but not to drop traffic. Because of this the term "IPS" is now commonly used to refer to both IDS and IPS. One way to think about IDS and IPS is that an IPS device that is deployed in-line (a "bump in the wire") is more capable of "preventing" an intrusion by dropping suspect packets, while an IPS deployed out-of-band (e.g. on a span port) can be thought of as an IDS, because it is monitoring mirrored network traffic, and can detect threats but is less able to prevent them. It may be the same make and model of network security device, but the way it is configured and deployed indicates whether it is a "passive" IDS or an "active" IPS.

Consider that the most basic definition of a firewall, given earlier, fails to provide the basic functionality recommended by NIST and other organizations, which advise filtering traffic on both the source and destination IP address and the associated service port, bidirectionally. At the same time, many modern firewalls are able to do much more—looking at whole application sessions rather than isolated network packets, by filtering application contents, and then enforcing filter rules that are sometimes highly complex. These unified threat management (UTM) appliances are becoming more common in protecting both industrial and business networks from today's advanced threats. Deploying a "firewall" may be inadequate for some installations while highly capable at others, depending upon the specific capabilities of the "firewall" and the particular threat that it is designed to protect the underlying system against. The various network-based cyber security controls that are available and relevant to industrial networks are examined in detail in Chapter 10, "Implementing Security and Access Controls" and Chapter 11, "Exception, Anomaly and Threat Detection."

INDUSTRIAL CONTROL SYSTEM

An industrial control system (ICS) is a broad class of automation systems used to provide control and monitoring functionality in manufacturing and industrial facilities. An ICS actually is the aggregate of a variety of system types including process control systems (PCS), distributed control systems (DCS), supervisory control and data acquisition (SCADA) systems, safety instrumented systems (SIS), and many others. A more detailed definition will be provided in Chapter 4, "Introduction to Industrial Control Systems and Operations."

Figure 2.1 is a simplified representation of an ICS consisting of two controllers and a series of inputs and outputs connecting to burners, valves, gauges, motors, and so on that all work in a tightly integrated manner to perform an automated task. The task is controlled by an application or logic running inside the controller, with local panels or human–machine interfaces (HMIs) used to provide a "view" into the controller allowing the operator to see values and make changes to how the controller is operating. The ICS typically includes toolkits for creating the process logic that defines the task, as well as toolkits for building custom operator interfaces or graphical user interfaces (GUIs) implemented on the HMI. As the task executes, the results are recorded in a database called an Historian (see Chapter 4, "Introduction to Industrial control Systems and Operations" for more information and detail on how such a system operates).

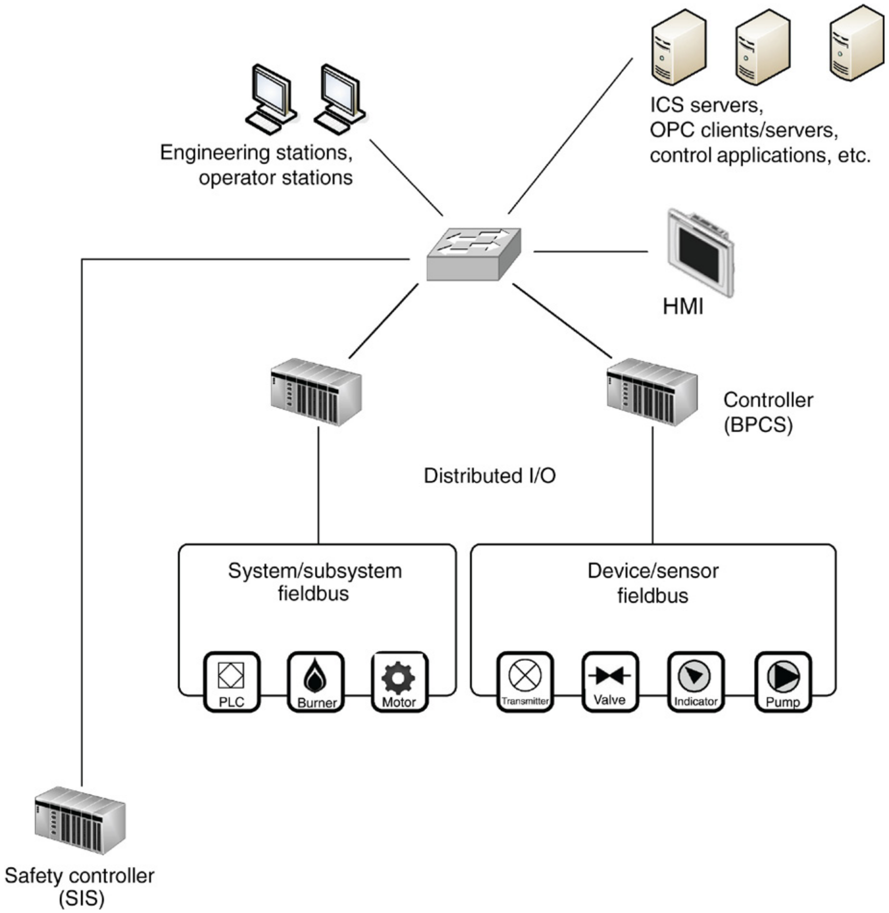


FIGURE 2.1 Sample industrial automation and control system.

DCS OR SCADA?

Originally, there were significant differences between the architectures of a DCS versus that of a SCADA system. As technology evolved, these differences have diminished, and there can often be a blur between whether a particular ICS is in fact classified as DCS or SCADA. Both systems are designed to monitor (reading data and presenting it to a human operator and possibly to other applications, such as historians and advanced control applications) and to control (defining parameters and executing instructions) manufacturing or industrial equipment. These system architectures vary by vendor, but all typically include the applications and tools necessary to generate, test, deploy, monitor, and control an automated process. These systems are multifaceted tools, meaning that a workstation might be used for purely supervisory (read only) purposes by a quality inspector, while another may be used to optimize process logic and write new programs for a controller, while yet a third may be used as a centralized user interface to control a process that requires more human intervention, effectively giving the workstation the role of the HMI.

It should be noted that ICSs are often referred to in the media simply as "SCADA," which is both inaccurate and misleading. Looking at this another way, a SCADA system is in fact an ICS, but not all ICSs are SCADA! The authors hope to help clarify this confusion in Chapter 4, "Introduction to Industrial Control Systems and Operations."

INDUSTRIAL NETWORKS

The various assets that comprise an ICS are interconnected over an Industrial Network. While the ICS represented in Figure 2.1 is accurate, in a real deployment the management and supervision of the ICS will be separated from the controls and the automation system itself. Figure 2.2 shows how an ICS is actually part of a much larger architecture, consisting of plant areas that contain common and shared applications, area-specific control devices, and associated field equipment, all interconnected via a variety of network devices and servers. In large or distributed architectures, there will be a degree of local and remote monitoring and control that is required (i.e. in the plant), as well as centralized monitoring and control (i.e. in the control room). This is covered in detail in Chapter 5, "Industrial Network Design and Architecture." For now it is sufficient to understand that the specialized systems that comprise an ICS are interconnected, and this connectivity is what we refer to as an Industrial Network.

INDUSTRIAL PROTOCOLS

Most ICS architectures utilize one or more specialized protocols that may include vendor-specific proprietary protocols (such as Honeywell CDA, General Electric SRTP or Siemens S7, and many others) or nonproprietary and/or licensed protocols including OPC, Modbus, DNP3, ICCP, CIP, PROFIBUS, and others. Many of these were originally designed for serial communications, but have been adapted to operate over standard Ethernet link layer using the Internet Protocol with both UDP and

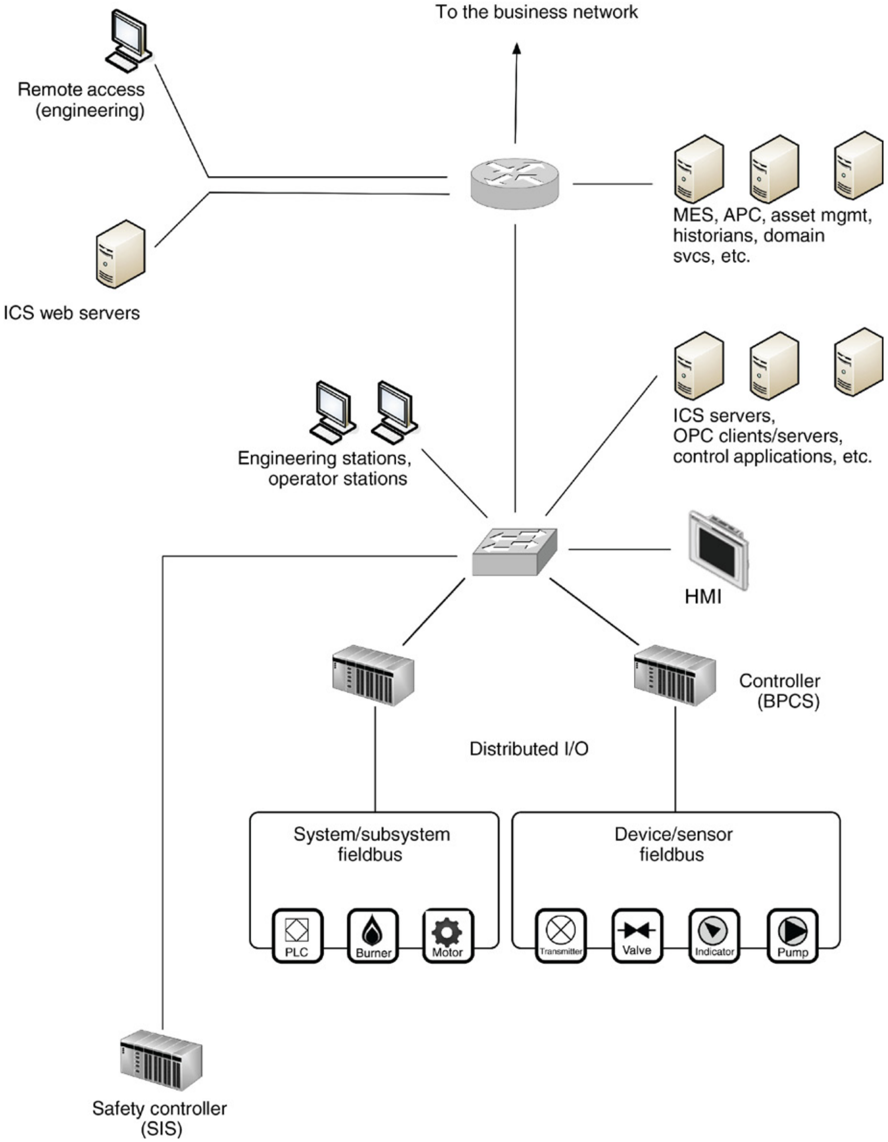

To the business network
Remote access (engineering)
ICS web servers
MES, APC, asset mgmt, historians, domain svcs, etc.
ICS servers, OPC clients/servers, control applications, etc.
Engineering stations, operator stations
HMI
Controller (BPCS)
Distributed I/O
System/subsystem fieldbus
PLC
Burner
Motor
Device/sensor fieldbus
Transmitter
Valve
Indicator
Pump
Safety controller (SIS)

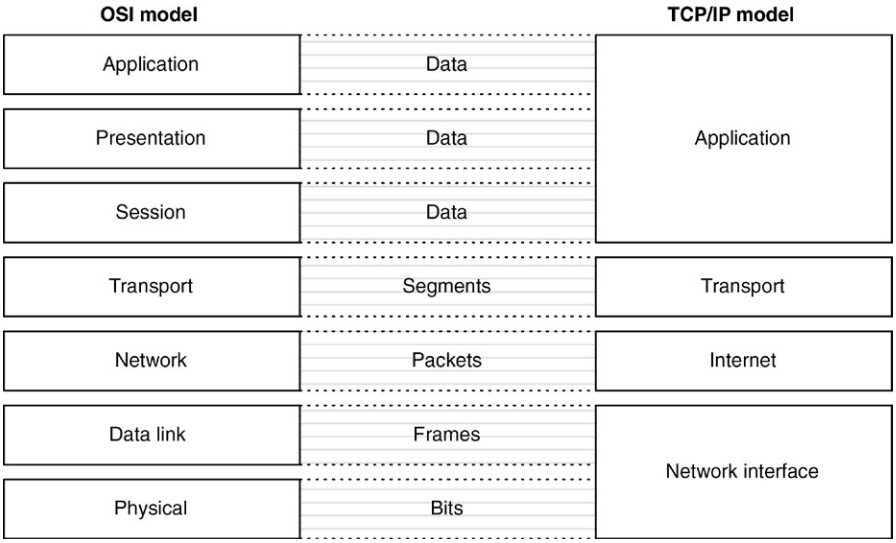
FIGURE 2.2 Sample network connectivity of an industrial control system.

TCP transports, and are now widely deployed over a variety of common network infrastructures. Because most of these protocols operate at the application layer, they can be accurately (and often are) referred to as applications. They are referred to as protocols in this book to separate them from the software applications that utilize them—such as DCS, SCADA, EMS, historians, and other systems.

THE OPEN SYSTEMS INTERCONNECTION (OSI) MODEL

The OSI model defines and standardizes the function of how a computing system interacts with a network. Each of seven layers is dependent upon and also serves the layers above and below it, so that information from an Application (defined at the topmost or Application Layer) can be consistently packaged and delivered over a variety of physical networks (defined by the bottommost or Physical Layer). When one computer wants to talk to another on a network, it must step through each layer: Data obtained from applications (Layer 7) are presented to the network (Layer 6) in defined sessions (Layer 5), using an established transport method (Layer 4), which in turn uses a networking protocol to address and route the data (Layer 3) over an established link (Layer 2) using a physical transmission mechanism (Layer 1). At the destination, the process is reversed in order to deliver the data to the receiving application. With the ubiquity of the Internet Protocol, a similar model called the TCP/IP Model is often used to simplify these layers. In the TCP/IP model, layers 5 through 7 (which all involve the representation and management of application data), and layers 1 and 2 (which define the interface with the physical network) are consolidated into a single Application Layer and Network Interface Layer. In this book we will reference the OSI model in order to provide a more specific indication of what step of the network communication process we are referring to (Figure 2.3).

Because these protocols were not designed for use in broadly accessible or public networks, cyber security was seen as compensating control and not an inherent requirement. Now, many years later, this translates to a lack of robustness that makes the protocols easily accessed—and in turn they can be easily broken, manipulated, or otherwise exploited. Some are proprietary protocols (or open protocols with many proprietary extensions, such as Modbus-PEMEX), and as such they have benefited for some time by the phenomena of "security by obscurity." This is clearly no longer



OSI model		TCP/IP model
Application	Data	Application
Presentation	Data	
Session	Data	
Transport	Segments	Transport
Network	Packets	Internet
Data link	Frames	Network interface
Physical	Bits	

FIGURE 2.3 The OSI and TCP/IP models.

the case with the broader availability of information on the World Wide Web, combined with an increasing trend of industry-focused cyber security research. Many of the concerns about industrial systems and critical infrastructure stem from the growing number of disclosed vulnerabilities within these protocols. One disturbing observation is that in the few years following the Stuxnet attack, many researchers have found numerous vulnerabilities with open protocol standards and the systems that utilize them. Little attention has been given to the potential problem of vulnerabilities in the proprietary products that are often times too cost prohibitive for traditional researchers to procure and analyze. These proprietary systems and protocols are at the core of most critical industry, and represent the greatest risk should they be compromised. See Chapter 6, "Industrial Network Protocols" and Chapter 7, "Hacking Industrial Systems" for more detail on these protocols, how they function, and how they can/have been compromised.

NETWORKS, ROUTABLE NETWORKS, AND NONROUTABLE NETWORKS

The differentiation between Routable and Nonroutable networks is becoming less common as industrial communications become more ubiquitously deployed over IP. A "nonroutable" network refers to those serial, bus, and point-to-point communication links that utilize **Modbus/RTU**, DNP3, fieldbus, and other networks. They are still networks—they interconnect devices and provide a communication path between digital devices, and in many cases are designed for remote command and control. A "routable" network typically means a network utilizing the Internet Protocol (TCP/IP or UDP/IP), although other routable protocols, such as AppleTalk, DECnet, Novell IPX, and other legacy networking protocols certainly apply. "Routable" networks also include routable variants of early "nonroutable" ICS protocols that have been modified to operate over TCP/IP, such as **Modbus over TCP/IP**, **Modbus/TCP**, and **DNP3 over TCP/UDP**. ICCP represents a unique case in that it is a relatively new protocol developed in the early 1990s, which allows both a point-to-point version and a wide-area routed configuration.

Routable and nonroutable networks would generally interconnect at the demarcation between the Control and Supervisory Control networks, although in some cases (depending upon the specific industrial network protocols used) the two networks overlap. This is illustrated in Figure 2.4 and is discussed in more depth in Chapter 5, "Industrial Control System Network Design and Architecture" and Chapter 6, "Industrial Network Protocols."

These terms were popularized through NERC CIP regulations, which implies that a routable interface can be easily accessed by the network either locally or remotely (via adjacent or public networks) and therefore requires special cyber security consideration; and inversely that nonroutable networks are "safer" from a network-based cyber-attack. This is misleading and can prevent the development of a strong cyber security posture. Today, it should be assumed that *all* industrial systems are connected either directly or indirectly to a "routable" network, whether or not they are connected via a routable protocol. Although areas of industrial

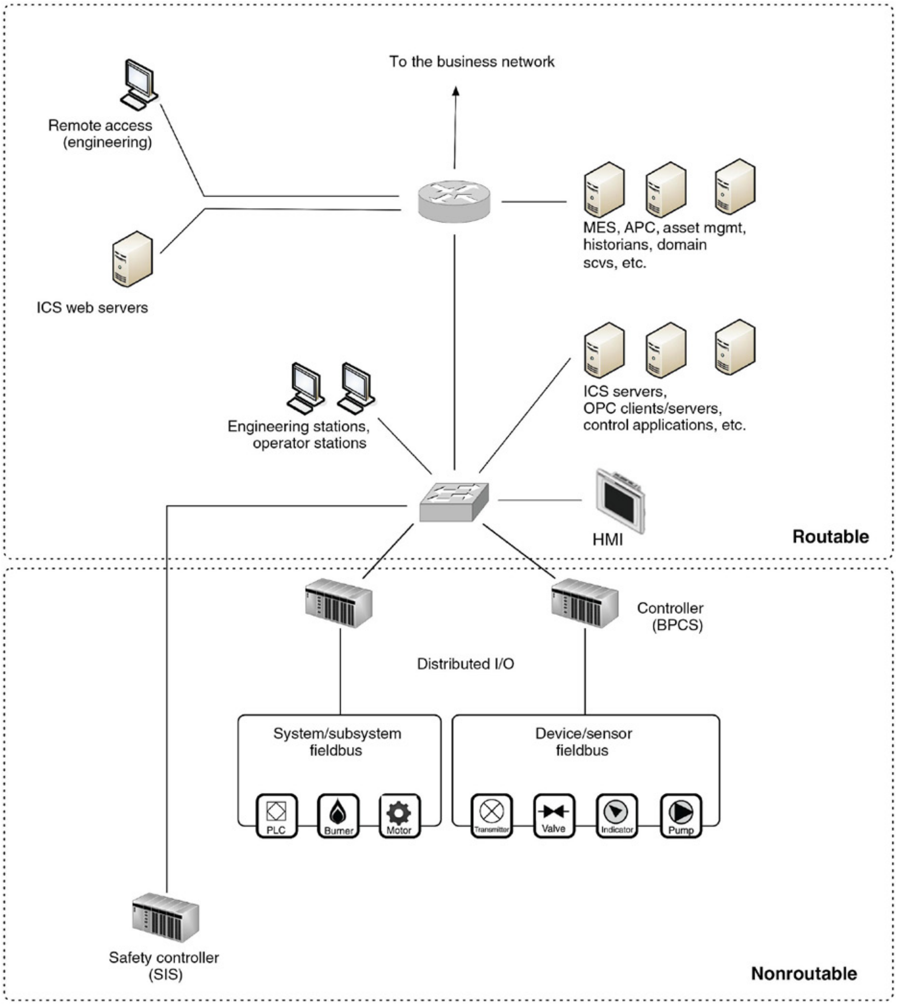

To the business network
Remote access (engineering)
ICS web servers
MES, APC, asset mgmt, historians, domain scvs, etc.
ICS servers, OPC clients/servers, control applications, etc.
Engineering stations, operator stations
HMI
Routable
Controller (BPCS)
Distributed I/O
System/subsystem fieldbus
Device/sensor fieldbus
PLC
Burner
Motor
Transmitter
Valve
Indicator
Pump
Safety controller (SIS)
Nonroutable

FIGURE 2.4 Routable and Nonroutable areas within an industrial control system.

networks may still be connected using serial or bus networks that operate via specific proprietary protocols, these areas can be accessed via other interconnected systems that reside on a larger IP network. For example, a PLC may connect to discrete I/O over legacy fieldbus connections. If considered in isolation, this would be a nonroutable network. However, if the PLC also contains an Ethernet uplink to connect to a centralized ICS system, the PLC can be accessed via that network and then manipulated to alter communications on the "nonroutable" connections. To further complicate things, many devices have remote access capabilities, such as modems, infrared receivers, radio or other connectivity options that may not be considered "routable" but are just as easily accessed by a properly equipped attacker. Therefore, the distinction between routable and nonroutable—though still widely used—is no longer considered a valid distinction by the authors. For the purposes of strong and cohesive cyber security practices, all networks and all devices should be considered potentially accessible and vulnerable. See Chapter 8, "Risk and Vulnerability Assessments" for more detail on determining accessibility and identifying potential attack vectors.

ENTERPRISE OR BUSINESS NETWORKS

An ICS is rarely an isolated system (in years of ICS design, we have found only a handful of examples of control systems that had no connectivity to any network). For every factory floor, electric generator, petroleum refinery, or pipeline, there is a corporation or organization that owns and operates the facility, a set of suppliers that provides raw materials, and a set of customers that receive the manufactured products. Like any other corporation or organization, these require daily business functions: sales, marketing, engineering, product management, customer service, shipping and receiving, finance, partner connectivity, supplier access, and so on. The network of systems that provide the information infrastructure to the business is called the business network.

There are many legitimate business reasons to communicate between the enterprise systems and industrial systems, including production planning and scheduling applications, inventory management systems, maintenance management systems, and manufacturing execution systems to name a few. The business network and the industrial network interconnect to make up a single end-to-end network.

Figure 2.5 illustrates this end-to-end functional network, as well as the separation of the business networks from the industrial networks, which consist of plant, supervisory, and functions. In this example, there is a high degree of redundancy in all areas, which is intended to make a point—the network infrastructure may be designed using the same "enterprise" switches and routers as those used in the business network. In some areas of an industrial network, "industrial" switches and routers may be used, which support harsher environments, offer higher availability, eliminate moving parts such as fans, and are otherwise engineered for "industrial" and sometimes "hazardous" use. In this book, the industrial network is defined by its function, not by the marketing designation provided by a product vendor, and so the supervisory network in Figure 2.4 is considered an industrial network even though it uses enterprise-class networking gear.

It should also be noted that there are several systems and services that exist in both business and industrial networks, such as directory services, file servers, and databases. These common systems should not be shared between business and industrial networks, but rather replicated in both environments in order to minimize the interconnectivity and reduce the potential attack surface of both the ICS and enterprise infrastructure.

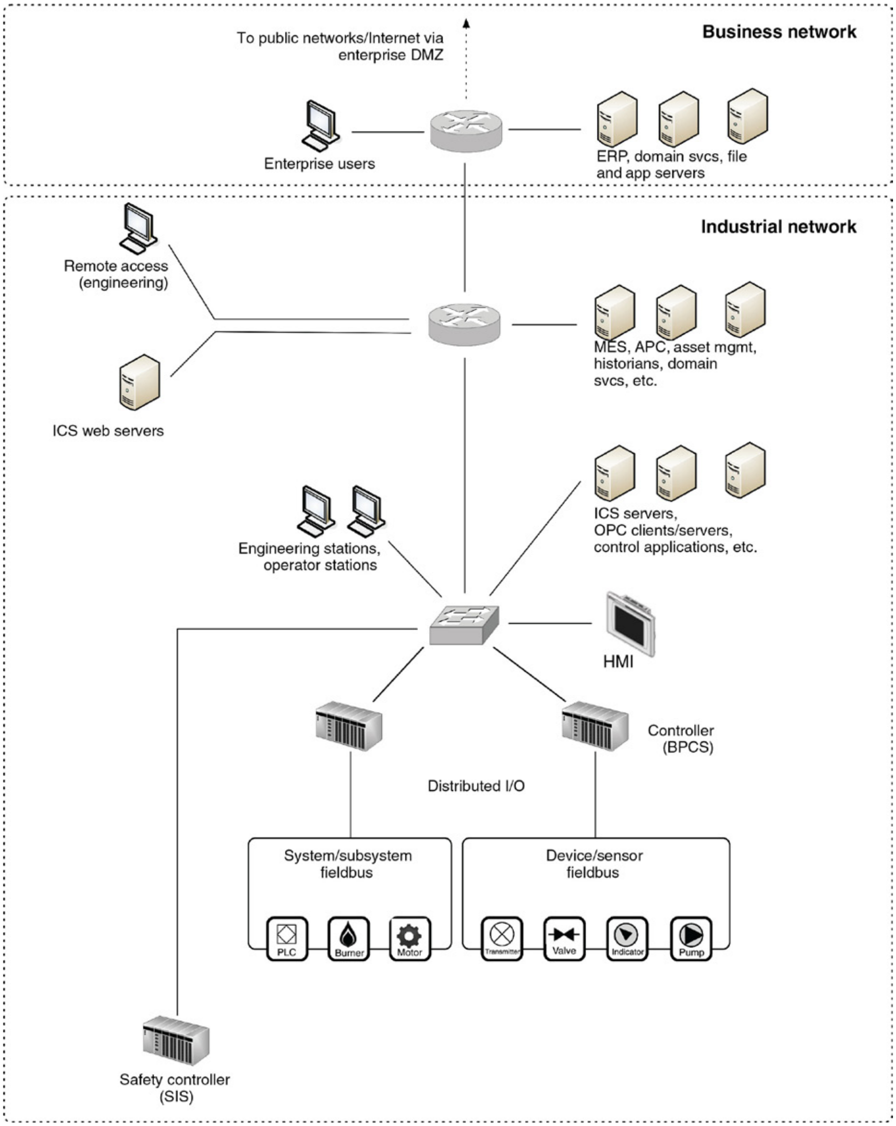

Business network
To public networks/Internet via enterprise DMZ
Enterprise users
ERP, domain svcs, file and app servers
Industrial network
Remote access (engineering)
MES, APC, asset mgmt, historians, domain svcs, etc.
ICS web servers
ICS servers, OPC clients/servers, control applications, etc.
Engineering stations, operator stations
HMI
Controller (BPCS)
Distributed I/O
System/subsystem fieldbus
Device/sensor fieldbus
PLC
Burner
Motor
Transmitter
Valve
Indicator
Pump
Safety controller (SIS)

FIGURE 2.5 Separation of business and industrial networks.

This book does not focus on the business network or its systems except where they might be used as an attack vector into the ICS. There are numerous books available on enterprise cyber security if more information is required on this subject. This book will also not focus on how internal attacks originating from the industrial network might be used to gain unauthorized access to business networks (this is a legitimate concern, but it is outside of the scope of this book).

ZONES AND ENCLAVES

The terms “enclave” and “zone” are convenient for defining a closed group of assets, or a functional group of devices, services, and applications that make up a larger system. While the term “enclave” is often used in the context of military systems, the term “zone” is now becoming more recognized, because it is referenced heavily within the widely adopted industry standards—ISA-62443 (formerly ISA-99). Originally developed from the Purdue Reference Model for Computer Integrated Manufacturing,[4] the concept of zones and conduits has now become widely adopted.

Within this model, communications are limited to only those devices, applications, and users that should be interacting with each other legitimately in order to perform a particular set of functions. Figure 2.6 shows zones as illustrated within IEC-62443, while Figure 2.7 then shows the same model applied to the sample network architecture used throughout this book.

The term “zone” is actually not new, but in fact has been used for many years in describing a special network that is created to expose a subset of resources (servers, services, applications, etc.) to a larger, untrusted network. This “demilitarized zone” or DMZ is typically used when enterprises want to place external-facing services, like web servers, email servers, B2B portals, and so on, on the Internet while still securing their more trusted business networks from the untrusted public Internet networks. It is important to note that at this point in the book, Figure 2.7 has been simplified and omits multiple DMZs that would typically be deployed to protect the Plant and Enterprise Zones.

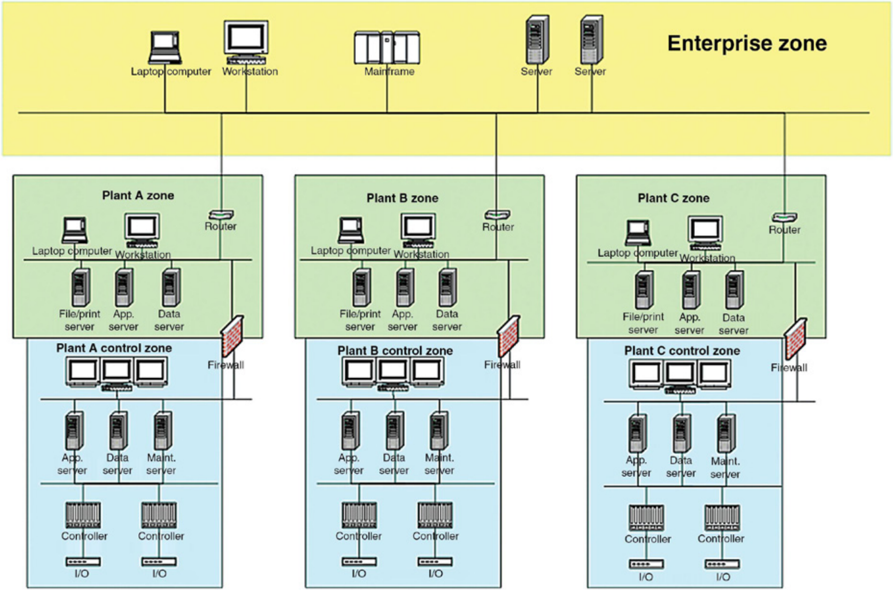


FIGURE 2.6 The ISA-62443 zone and conduit model (block diagram).

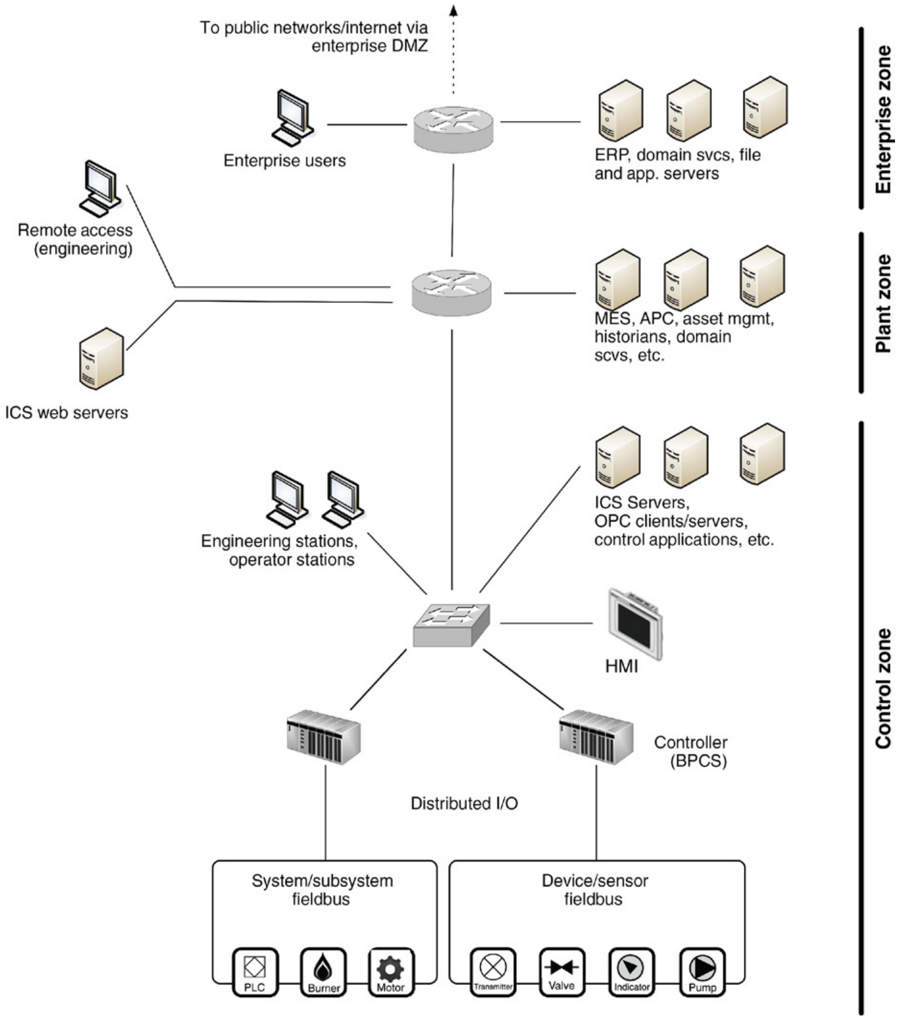

To public networks/internet via enterprise DMZ
Enterprise users
ERP, domain svcs, file and app. servers
Enterprise zone
Remote access (engineering)
MES, APC, asset mgmt, historians, domain scvs, etc.
Plant zone
ICS web servers
ICS Servers, OPC clients/servers, control applications, etc.
Engineering stations, operator stations
HMI
Controller (BPCS)
Distributed I/O
Control zone
System/subsystem fieldbus
Device/sensor fieldbus
PLC
Burner
Motor
Transmitter
Valve
Indicator
Pump

FIGURE 2.7 The ISA-62443 zone and conduit model (network diagram).

While highly effective when properly implemented, zones and conduits can become difficult to engineer and to manage in more distributed, complex systems. For example, in a simple control loop, an HMI interfaces with a PLC that interacts with sensors and actuators to perform a specific control function. The "Plant Control Zone" in Figure 2.6 includes all devices within the control loop including the PLC and an HMI. Because the authorized users allowed to operate the HMI may not be physically located near these devices, a "conduit" enforces appropriate authentication and authorization (and potentially monitoring or accounting) between the user and resources. This can be exasperating when systems grow in both size and complexity, such as in a Smart Grid architecture. Smart Grids are highly complex and highly interconnected, as evident in Figure 2.8, making it difficult to adequately separate systems into security zones. For more on the zone and conduit model and how to apply it to real industrial control environments, see Chapter 9, "Establishing Zones and Conduits."

NOTE

Zone and conduits are a method of **network segregation**, or the separation of networks and assets in order to enforce and maintain access control. A zone does not necessarily require a physical boundary, but it does require a logical delineation of systems (i.e. assets combined with the communication conduits that exist between them). Zones are an important aspect of cyber security as they define acceptable versus unacceptable access to the various systems and subsystems that comprise an ICS that are placed within a particular zone. Though many standards may not specifically mention zones, most describe the concept of segmentation as one of the fundamental network security controls. Zones and conduits are typically the outcome of this network segmentation activity. The mapping and management of zones can become confusing because a single asset could exist in multiple logical zones. The concept of zones is expanded further in Chapter 9, "Establishing Zones and Conduits," but for now it is enough to understand the term and how it will be used.

NETWORK PERIMETERS OR "ELECTRONIC SECURITY PERIMETERS"

The outermost boundary of any closed group of assets (i.e. a "zone") is called the perimeter. The perimeter is a point of demarcation between what is outside of a zone, and what is inside. A perimeter is a logical point at which to implement cyber security controls. One hidden aspect of creating a perimeter is that it provides a means to implement controls on devices that may not support the direct implementation of a particular control. This concept will be explained further later in this book.

NERC CIP popularized the terminology "Electronic Security Perimeter" or "ESP" referring to the boundary between secure and insecure zones.[5] The perimeter itself is nothing more than a logical "dotted line" around that separates the closed group of assets within its boundaries from the rest of the network. "Perimeter defenses" are the security defenses established to police the entry into or out of the different zones, and typically consist of firewalls, intrusion prevention system, or similar network-based filters. This is discussed in depth in Chapter 9, "Establishing Zones and Conduits."

NOTE: PERIMETER SECURITY AND THE CLOUD

When dealing with well-defined, physically segmented and demarcated networks, perimeters are easily understood and enforced. However, as more and more remote systems become interconnected, often relying on shared resources stored in a central data center, a perimeter becomes more difficult to define and even more difficult to enforce. A Smart Grid, for example, may utilize broadly distributed measurement devices throughout the transmission and distribution grid, all of which interact with a centralized service. This is an example of Private Cloud Computing, and it comes with all of the inherent risks and concerns of cloud-based computing. For more information about Cloud Computing, please refer to the "CSA Guide to Cloud Computing" by Raj Samani, Brian Honan, and Jim Reavis, published by Elsevier.

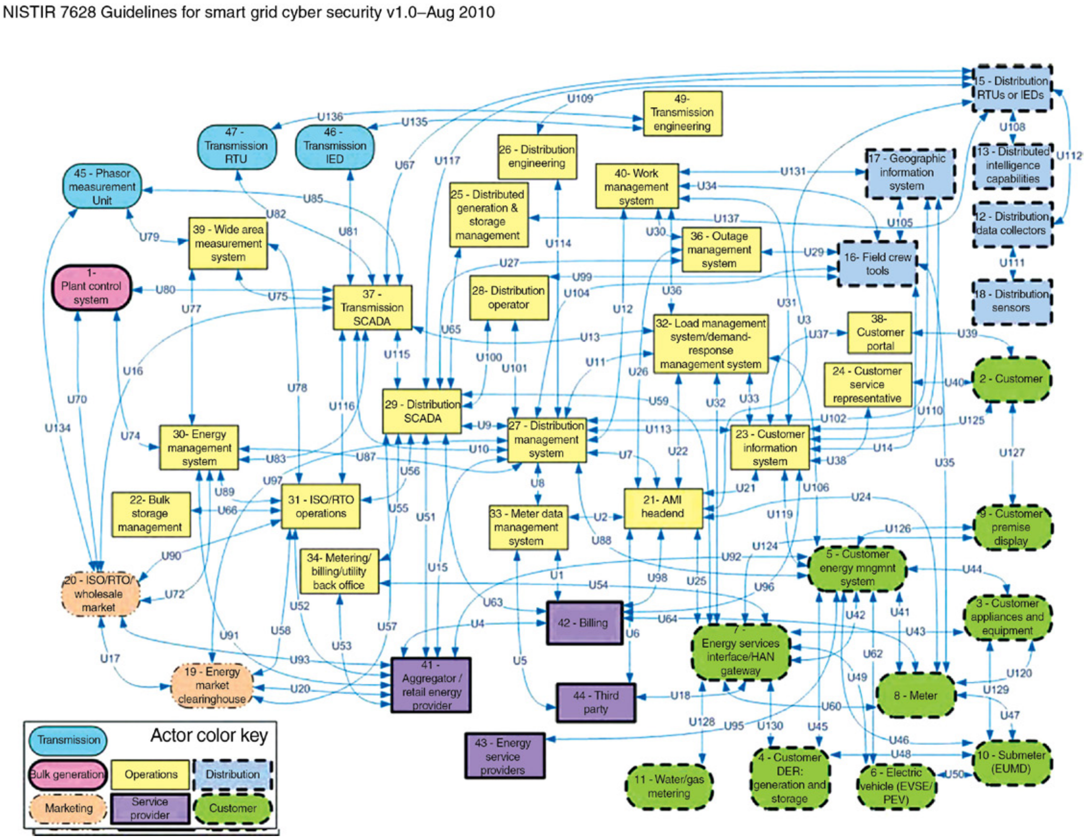

NISTIR 7628 Guidelines for smart grid cyber security v1.0–Aug 2010
15 - Distribution RTUs or IEDs
49- Transmission engineering
47 - Transmission RTU
46 - Transmission IED
26 - Distribution engineering
45 - Phasor measurement Unit
40- Work management system
17 - Geographic information system
13 - Distributed intelligence capabilities
25 - Distributed generation & storage management
39 - Wide area measurement system
36 - Outage management system
12 - Distribution data collectors
16- Field crew tools
1- Plant control system
37 - Transmission SCADA
28- Distribution operator
18 - Distribution sensors
32- Load management system/demand-response management system
38- Customer portal
24 - Customer service representative
2 - Customer
29 - Distribution SCADA
27 - Distribution management system
30- Energy management system
23 - Customer information system
22- Bulk storage management
31 - ISO/RTO operations
33 - Meter data management system
21- AMI headend
9 - Customer premise display
34- Metering/ billing/utility back office
5 - Customer energy mngmnt system
20 - ISO/RTO/ wholesale market
42 - Billing
3 - Customer appliances and equipment
7 - Energy services interface/HAN gateway
19 - Energy market clearinghouse
41 - Aggregator / retail energy provider
44 - Third party
8 - Meter
43 - Energy service providers
11 - Water/gas metering
4 - Customer DER: generation and storage
6 - Electric vehicle (EVSE/ PEV)
10 - Submeter (EUMD)
Actor color key
Transmission
Bulk generation
Operations
Distribution
Marketing
Service provider
Customer

FIGURE 2.8 The challenge of applying zones to the Smart Grid (From NISTIR 7628).

CRITICAL INFRASTRUCTURE

For the purposes of this book, the terms "Industrial Network" and "Critical Infrastructure" are used in somewhat limited contexts. Herein, "Industrial Network" is referring to any network operating some sort of automated control system that communicates digitally over a network, and "Critical Infrastructure" is referring to the critical *systems and assets* used within a networked computing infrastructure. Confusing? It is, and this is perhaps one of the leading reasons that many critical infrastructures remain at risk today; many ICS security seminars have digressed into an argument over semantics, at the sake of any real discussion on network security practices.

Luckily, the two terms are closely related in that the defined critical *national* infrastructures, meaning those systems listed in the **Homeland Security Presidential Directive Seven** (**HSPD-7**), typically utilizes some sort of industrial control systems. In its own words, "HSPD-7 establishes a national policy for Federal departments and agencies to identify and prioritize [the] United States critical infrastructure[s] and key resources and to protect them from terrorist attacks." HSPD-7 includes public safety, bulk electric energy, nuclear energy, chemical manufacturing, agricultural and pharmaceutical manufacturing and distribution, and even aspects of banking and finance—basically, anything whose disruption could impact a nation's economy, security, or health.[6] While financial services, emergency services, and health care are considered a part of our critical national infrastructure, they do not typically directly operate industrial control networks, and so are not addressed within this book (although many of the security recommendations will still apply, at least at a high level).

Utilities

Utilities—water, wastewater, gas, oil, electricity, and communications—are critical national infrastructures that rely heavily on industrial networks and automated control systems. Because the disruption of any of the systems associated with these infrastructures could impact our society and our safety, they are listed as critical by HSPD-7. They are also clear examples of industrial networks, because they use automated and distributed process control systems. Of the common utilities, electricity is often separated as requiring more extensive security. In the United States and Canada, it is specifically regulated to standards of reliability and cyber security. Petroleum refining and distribution are systems that should be treated as both a chemical/hazardous material and as a critical component of our infrastructures, but at the time this book was published were not directly regulated by federal authorities for cyber security compliance in a manner similar to NERC CIP.

Nuclear Facilities

Nuclear facilities represent unique safety and security challenges due to their inherent danger in fueling and operation, as well as the national security implications of the raw materials used. These plants typically comprise a base load contribution to the national electric grid. This makes nuclear facilities a prime target for cyber-attacks, and makes the consequences of a successful attack more severe. The **Nuclear Regulatory Commission** (**NRC**), as well as NERC and the Federal Energy Regulatory Commission (FERC), heavily regulate nuclear energy in the United States when it comes to supplying electricity to the grid. Congress formed the NRC as an independent agency in 1974 in an attempt to guarantee the safe operation of nuclear facilities and to protect people and the environment. This includes regulating the use of nuclear material including by-product, source, and special nuclear materials, as well as nuclear power.[7]

Bulk Electric

The ability to generate and transmit electricity in bulk is highly regulated. Electrical energy generation and transmission is defined as critical infrastructures under HSPD-7, and is heavily regulated in North America by **NERC**—specifically via the NERC CIP reliability standards—under the authority of the Department of Energy (DoE). The DoE is also ultimately responsible for the security of the production, manufacture, refining, distribution, and storage of petroleum, natural gas, and nonnuclear electric power.[8]

It is important to note that energy generation and transmission are two distinct industrial network environments, each with its own nuances and special security requirements. Energy generation is primarily concerned with the safe manufacture of a product (electricity), while energy transmission is concerned with the safe and balanced transportation of that product. The two are also highly interconnected, obviously, as generation facilities directly feed the power grid that distributes that energy, since bulk energy must be carefully measured and distributed upon production. For this same reason, the trading and transfer of power between power companies is an important facet of an electric utility's operation and the stability of the grid at large.

The Smart Grid—an update to traditional electrical transmission and distribution systems to accommodate digital communications for metering and intelligent delivery of electricity—is a unique facet of industrial networks that is specific to the energy industry, which raises many new security questions and concerns.

Although energy generation and transmission are not the only industrial systems that need to be defended, they are often used as examples within this book. This is because NERC has created the CIP reliability standard and enforces it heavily throughout the United States and Canada. Likewise, the NRC requires and enforces the cyber security of nuclear power facilities. Ultimately, all other industries rely upon electric energy to operate, and so the security of the energy infrastructure (and the development of the Smart Grid) impacts everything else. Talking about securing industrial networks without talking about energy is practically impossible.

Is bulk power more important than the systems used in other industry sectors? That is a topic of heavy debate. Within the context of this book, we assume that all control systems are important, whether or not they generate or transmit energy, or whether they are defined that way by HSPD-7 or any other directive. A speaker at the 2010 Black Hat conference suggested that ICS security is overhyped, because these systems are more likely to impact the production of cookies than they are to impact our national infrastructure.[9] Even the production of a snack food can impact many lives—through the manipulation of its ingredients or through financial impact to the producer and its workers and the communities in which they live. What is important to realize here is that the same industrial systems are used across designated "critical" and "noncritical" national infrastructures—from making cookies to making electrical energy.

Smart Grid

The Smart Grid is a modernization of energy transmission, distribution, and consumption systems. A Smart Grid improves upon legacy systems through the addition of monitoring, measurement, and automation—allowing many benefits to energy producers (through accurate demand and response capabilities for energy generation), energy providers (through improved transmission and distribution management, fault isolation and recovery, metering and billing, etc.), and energy consumers (through in-home energy monitoring and management, support for alternate energy sources, such as home generation or electric vehicle charge-back, etc.). The specific qualities and benefits of the Smart Grid are far too extensive and diverse to list them all herein. The Smart Grid is used extensively within this book as an example of how an industrial system—or in this case a "system of systems"—can become complex, and as a result become a large and easy target for a cyber-attacker.

This is partly because by becoming "smart," the devices and components that make up the transmission, distribution, metering, and other components of the grid infrastructure have become sources of digital information (representing a privacy risk), have been given distributed digital communication capability (representing a cyber-security risk), and have been highly automated (representing a risk to reliability and operations should a cyber-attack occur). In "Applied Cyber Security and the Smart Grid," the Smart Grid is described using an analogy of human biology: the increased monitoring and measurement systems represents the eyes, ears, and nose as well as the sensory receptors of the brain; the communication systems represents the mouth, vocal chords, eyes, and the ears, as well as the communicative center of the brain; and the automation systems represent the arms, hands, and fingers, as well as the motor functions of the brain. The analogy is useful because it highlights the common participation of the brain—if the Smart Grid's brain is compromised, all aspects of sensory perception, communication, and response can be manipulated.

The Smart Grid can be thought of within this book as a more complex "system of systems" that is made up of more than one industrial network, interconnected to provide end-to-end monitoring, analytics, and automation. The topics discussed herein apply to the Smart Grid even though they may be represented in a much simpler form. Some of the differences in Smart Grid architecture and operations are covered in Chapter 5, "Industrial Network Design and Architecture" and in more detail in the complimentary publication "Applied Cyber Security and the Smart Grid."

Chemical Facilities

Chemical manufacture and distribution represent specific challenges to securing an industrial manufacturing network. Unlike the "utility" networks (electric, water, wastewater, natural gas, fuels), chemical facilities need to secure their intellectual property as much as they do their control systems and manufacturing operations. This is because the product itself has a tangible value, both financially and as a weapon. For example, the formula for a new pharmaceutical could be worth a large sum of money on the black market. The disruption of the production of that pharmaceutical could be used as a social attack against a country or nation, by impacting the ability to produce a specific vaccine or antibody. Likewise, the theft of hazardous chemicals can be used directly as weapons or to fuel illegal chemical weapons research or manufacture. Chemical facilities need to also focus on securing the storage and transportation of the end product for this reason.

COMMON INDUSTRIAL SECURITY RECOMMENDATIONS

Many of the network security practices that are either required or recommended by the aforementioned organizations are consistent between many if not all of the others. Although all recommendations should be considered, these common "best practices" are extremely important and are the basis for many of the methods and techniques discussed within this book. They consist of the following steps:

1. Identifying what systems need to be protected,
2. Separating the systems logically into functional groups,
3. Implementing a defense-in-depth strategy around each system or group,
4. Controlling access into and between each group,
5. Monitoring activities that occur within and between groups, and
6. Limiting the actions that can be executed within and between groups.

IDENTIFICATION OF CRITICAL SYSTEMS

The first step in securing any system is determining what needs to be protected, and this is reflected heavily in NERC CIP, NRC 10 CFR 73.54, and ISA-62443. Identifying the assets that need to be secured, as well as identifying their individual importance to the reliable operation of the overall integrated system, is necessary for a few primary reasons. First, it tells us what should be monitored, and how closely. Next, it tells us how to logically segment the network into high-level security zones. Finally, it indicates where our point security devices (such as firewalls and intrusion protection systems) should be placed. For North American electric companies, it also satisfies a direct requirement of NERC CIP, and therefore can help to minimize fines associated with noncompliance.

Identifying critical systems is not always easy. The first step is to build a complete inventory of all connected devices in terms of not only the physical asset itself, but also the logical assets that reside within. Remember that in the end, cyber security controls will be applied to protect specific logical assets, so it is important to adequately define them at this early stage. For example, an Active Directory server that performs the File and Storage Services role and therefore contains the "files" as a logical asset is different from another AD server that is assigned the Domain Services roles and contains "credentials" as one of its logical asset. Each of these devices should be evaluated independently. If it performs a critical function, it should be classified as critical. If it does not, consider whether it could impact any other critical devices or operations. Could it impact the network itself, preventing another device from interacting with a critical system and therefore causing a failure? Finally, does it protect a critical system in any way?

The NRC provides a logic map illustrating how to determine critical assets, which is adapted to more generic asset identification in Figure 2.9. This process will help to separate devices into two categories:

- Critical Assets
- Noncritical Assets

In many larger operations, this process may be over simplified. There may be different levels of "criticality" depending upon the individual goals of the operational process, the operating company, and even the nation within which that company is incorporated. A general rule to follow once the basic separation of critical versus noncritical has been completed is as follows. Are there any critical assets that are not functionally related to other critical assets? If there are, next ask if one function is more or less important than the other. Finally, if there is both a functional separation *and* a difference in the criticality of the system, consider adding a new logical "tier" to your network. Also remember that a device could potentially be critical *and* also directly impact one or more other critical assets. Consider ranking the criticality

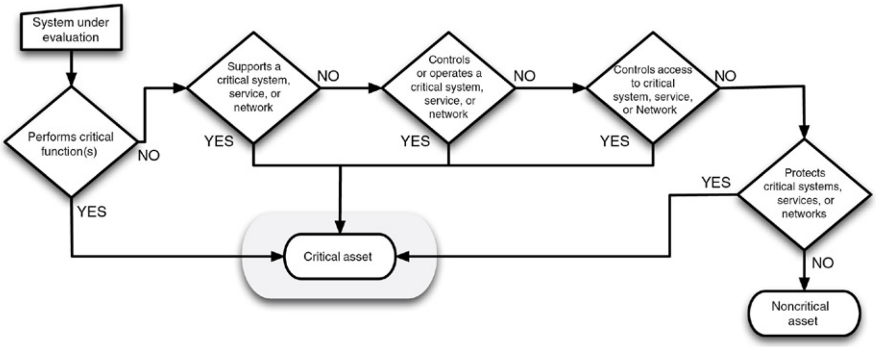

System under evaluation
Performs critical function(s)
NO
YES
Supports a critical system, service, or network
NO
YES
Controls or operates a critical system, service, or network
NO
YES
Controls access to critical system, service, or Network
NO
YES
YES
Protects critical systems, services, or networks
NO
Critical asset
Noncritical asset

FIGURE 2.9 NRC process diagram for identifying critical cyber assets.[10]

of devices based on their total impact to the overall system as well. Each layer of separation can then be used as a point of demarcation, providing additional layers of defense between each group.

NETWORK SEGMENTATION/ISOLATION OF SYSTEMS

The separation of assets into functional groups allows specific services to be tightly locked down and controlled, and is one of the easiest methods of reducing the attack surface that is exposed to potential threat actors. It is possible to eliminate most of the vulnerabilities—known or unknown—that could potentially allow an attacker to exploit those services simply by disallowing all unnecessary services and communication ports.

For example, if several critical services are isolated within a single functional group and separated from the rest of the network using a single firewall, it may be necessary to allow several different traffic profiles through that firewall (see Figure 2.10). If an attack is made using an exploit against web services over port 80/tcp, that attack may compromise a variety of services including e-mail services, file transfers, and patch/update services.

However, if each specific service is grouped functionally and separated from all other services, as shown in Figure 2.11—that is, all patch services are grouped together in one group, all database services in another group, and so on—the firewall can be configured to disallow anything other than the desired service, preventing an update server using HTTPS from being exposed to a threat that exploits a weakness in SQL on the database servers. Applying this to the reference design, it is easy to see how additional segmentation can protect attacks from pivoting between centrally located services. This is the fundamental concept behind the design of what are called "functional DMZs."

In an industrial control system environment, this method of service segmentation can be heavily utilized because there are many distinct functional groups within an industrial network that should not be communicating outside of established

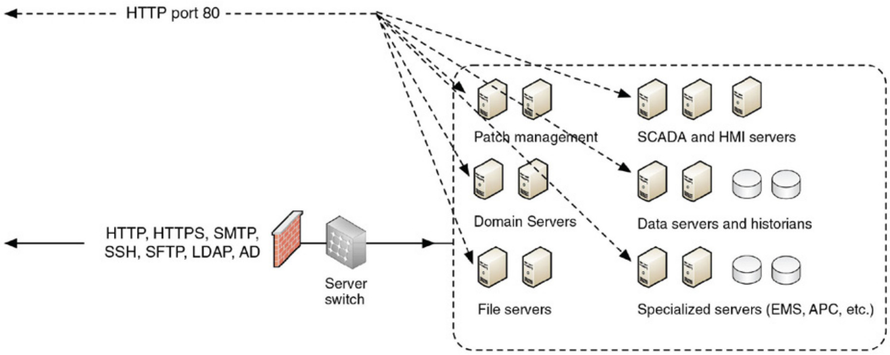

HTTP port 80
Patch management
SCADA and HMI servers
Domain Servers
Data servers and historians
HTTP, HTTPS, SMTP, SSH, SFTP, LDAP, AD
Server switch
File servers
Specialized servers (EMS, APC, etc.)

FIGURE 2.10 Placing all services behind a common defense provides a broader attack surface on all systems.

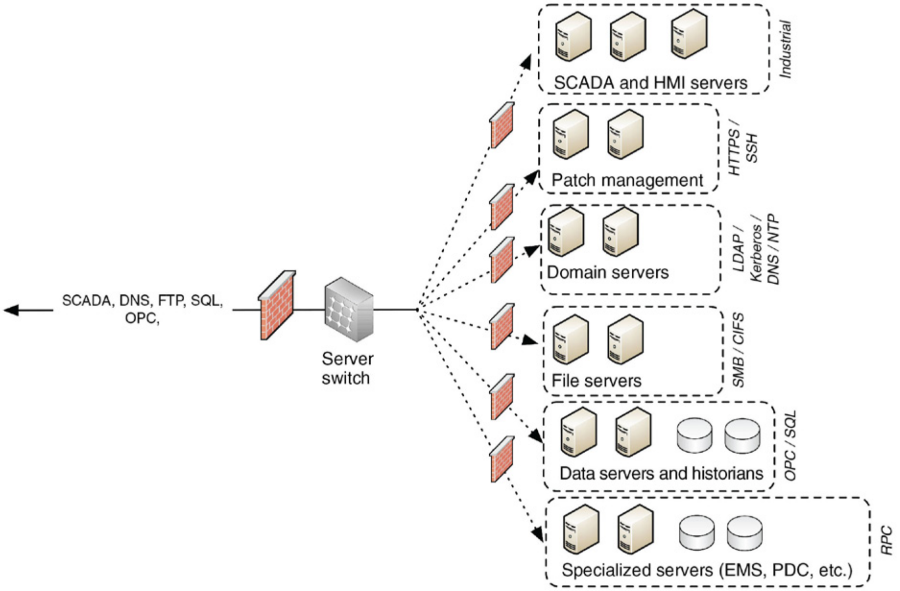


FIGURE 2.11 Separation into functional groups reduces the attack surface to a given system.

parameters. For example, protocols such as Modbus or DNP3 (discussed in depth in Chapter 6, "Industrial Network Protocols") are specific to ICSs and should never be used within the business network, while Internet services, such as HTTP, IMAP/POP, FTP, and others, should never be used within supervisory or control network areas. In Figure 2.12 it can be seen how this layered approach to functional and topological isolation can greatly improve the defensive posture of the network.

These isolated functional zones are often depicted as being separated by a firewall that interconnects them by conduits with other zones within this book. In many cases, a separate firewall may be needed for each zone. The actual method of securing the zone can vary and could include dedicated firewalls, intrusion protection devices, application content filters, access control lists, and/or a variety of other controls. Multiple zones can be supported using a single firewall in some cases through the careful creation and management of policies that implicitly define which hosts can connect over a given protocol or service port. This is covered in detail in Chapter 9, "Establishing Zones and Conduits."

CAUTION

Do not forget to control communications in both directions through a firewall. Not all threats originate from outside to inside (less trusted to more trusted networks). Open, outbound traffic policies can facilitate an insider attack, enable the internal spread of malware, enable outbound command and control capabilities, or allow for data leakage or information theft.

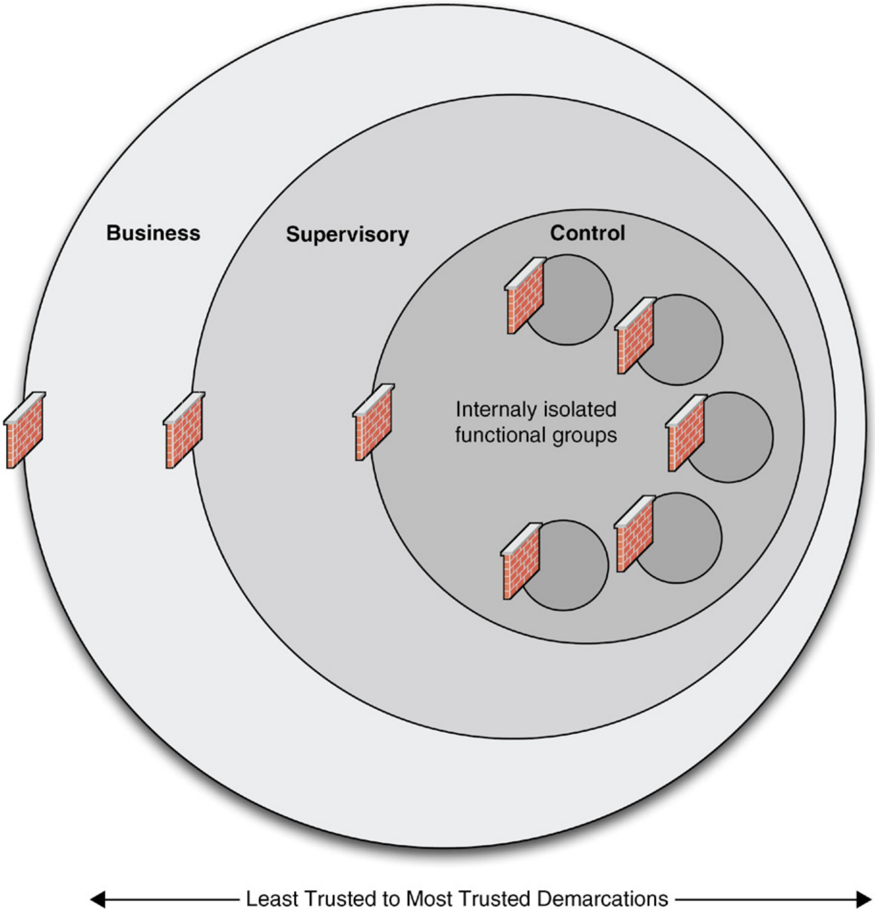

Business
Supervisory
Control
Internaly isolated functional groups
Least Trusted to Most Trusted Demarcations

FIGURE 2.12 Topological defense in depth provides additional layers of protection.

DEFENSE IN DEPTH

All standards organizations, regulations, and recommendations indicate that a defense-in-depth strategy should be implemented. The philosophy of a layered or tiered defensive strategy is considered a best practice even though the definitions of “defense in depth” can vary somewhat from document to document. Figure 2.13 illustrates a common defense-in-depth model, mapping logical defensive levels to common security tools and techniques.

The term “defense in depth” can and should be applied in more than one context because of the segregated nature of most industrial systems, including

- The layers of the Open Systems Interconnection (OSI) model, from physical (Layer 1) to Application (Layer 7).
- Physical or Topological layers consisting of subnetworks and/or functional zones.

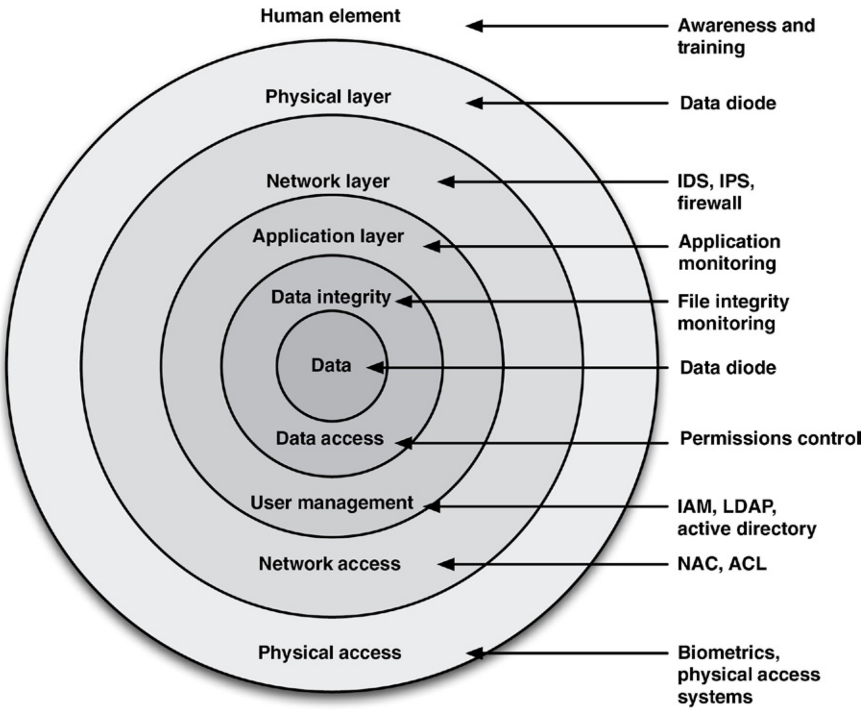


FIGURE 2.13 Defense in depth with corresponding protective measures.

- Policy layers, consisting of users, roles, and privileges.
- Multiple layers of defensive devices at any given demarcation point (such as implementing a firewall and an intrusion prevention system).

ACCESS CONTROL

Access control is one of the most difficult yet important aspects of cyber security. Access control considers three very important aspects of how a user interacts with resources (e.g. local application, and remote server). These aspects are identification, authentication, and authorization. It becomes more difficult for an attacker to identify and exploit systems by locking down services to specific users or groups of users accessing specific resources. The further access can be restricted, the more difficult an attack becomes. Although many proven technologies exist to enforce access control, the successful implementation of access control is difficult because of the complexity of managing users and their roles and their mapping to specific devices and services that relate specifically to an employee's operational responsibilities. As shown in Table 2.1, the strength of access control increases as a user's identity is treated with the additional context of that user's roles and responsibilities within a functional group.

Table 2.1 Adding Context to User Authentication to Strengthen Access Control

Good	Better	Best
User accounts are classified by authority level	User accounts are classified by functional role	User accounts are classified by functional role and authority
Assets are classified in conjunction with user authority level	Assets are classified in conjunction with function or operational role	Assets are classified in conjunction with function and user authority
Operational controls can be accessed by any device based on user authority	Operational controls can be accessed by only those devices that are within a functional group	Operational controls can only be accessed by devices within a functional group by a user with appropriate authority

Again, the more layers of complexity applied to the user rules, the more difficult it will be to gain unauthorized access. Some examples of advanced access control include the following:

- Only allow a user to log in to an HMI if the user has successfully badged into the control room (user credentials combined with physical access controls—station-based access control)
- Only allow a user to operate a given control from a specific controller (user credentials limited within a security zone—area of responsibility)
- Only allow a user to authenticate during that user's shift (user credentials combined with personnel management—time-based access control)

TIP

Authentication based on a combination of multiple and unrelated identifiers provides the strongest access control, for example, the use of both a digital and a physical key, such as a password and a biometric scanner. Another example may include the use of dedicated hosts for specific functions. The specific purpose of each ICS component under evaluation must be considered, and account for unique operational requirements of each. It may be possible to implement strong, multifactor authentication at an Engineering Workstation, where this may not be acceptable at an Operator HMI that depends on shared operator accounts.

ADVANCED INDUSTRIAL SECURITY RECOMMENDATIONS

The cyber security industry evolves rapidly and newer security products and technologies are being introduced every day—certainly faster than they can be referenced or recommended by standards and other industry organizations. Some advanced security recommendations include real-time activity and event monitoring using a Security Information and Event Management system (SIEM), network-based anomaly detection tools, policy whitelisting using an industrial firewall or industrial protocol filter, end-system malware protection using application whitelisting, and many others. There are undoubtedly new security products available since the time of this writing—it is good advice to always research new and emerging security technology when designing, procuring, or implementing new cyber security measures.

SECURITY MONITORING

Monitoring an information technology system is a recognized method of providing situational awareness to a cyber-security team, and monitoring tools, such as SIEM and Log Management systems, are heavily utilized by enterprise IT departments for this reason. Improved situational awareness can also benefit industrial networks, although special care needs to be taken in determining what to monitor, how to monitor it, and what the information gathered means in the context of cyber security. For more detail on how to effectively monitor an industrial network, see Chapter 12, "Security Monitoring of Industrial Control Systems."

POLICY WHITELISTING

"Blacklists" define what is "bad" or not allowed—malware, unauthorized users, and so on. A "whitelist" is a list of what is "good" or what is allowed—authorized users, approved resources, approved network traffic, safe files, and so on. A policy whitelist defines the behavior that is acceptable. This is important in ICS architectures, where an industrial protocol is able to exhibit specific behaviors, such as issuing commands, collecting data, or shutting down a system. A policy whitelist, also referred to as a protocol whitelist, understands what industrial protocol functions are allowed and prevents unauthorized behaviors from occurring. Policy whitelisting is a function that is available to newer and more advanced industrial firewalls. This is discussed in more detail in Chapter 11, "Exception, Anomaly and Threat Detection."

APPLICATION WHITELISTING

Application whitelisting defines the applications (and files) that are known to be "good" on a given device, and prevents any other applications from executing (or any other file from being accessed). This is an extremely effective deterrent against malware, since only advanced attacks directed against resident memory of an end system have the ability to infect systems with properly implemented application whitelisting. This also helps improve resilience of those systems that are not actively patched either due to operational issues or vendor specifications. This is discussed in more detail in Chapter 11, "Exception, Anomaly and Threat Detection."

COMMON MISPERCEPTIONS ABOUT INDUSTRIAL NETWORK SECURITY

In any discussion about industrial cyber security, there is always going to be objections from some that are based on misperceptions. The most common are

- *Cyber security of industrial networks is not necessary*. The myth remains that an "air gap" separates the ICS from any possible source of digital attack or infection. This is simply no longer true. While network segmentation is a valuable method for establishing security zones and improving security, the absolute separation of networks promised by the air gap is virtually impossible to obtain. "Air" is not an adequate defense against systems that support wireless diagnostics ports, removable media that can be hand-carried, and so on. This myth also assumes that all threats originate from outside the industrial network, and fails to address the risk from the insider and the resulting impact of a cyber-event on the ICS from an authorized user. This is a religious debate to some. To the authors of this book, the air gap is a myth that must be dispelled if cyber security is to be taken seriously.
- *Industrial security is an impossibility*. Security requires patching. Devices need to be patched to protect against the exploitation of a discovered vulnerability, and anti-virus systems need regular updates. Control environments cannot support adequate patch cycles, making any cyber security measures moot. While it is true that these are challenges faced in ICSs, it does not mean that a strong security posture cannot be obtained through other compensating controls. Industrial security requires a foundation of risk management and an understanding of the security lifecycle.
- *Cyber security is someone else's responsibility*. This comment is typically heard from plant operational managers hoping that IT managers will adopt responsibility (and budget) for cyber security. It is more often than not in operations' benefit to take responsibility for cyber security. Cyber security will have ownership at the highest executive levels in a properly structured organization, and appropriate responsibilities will trickle down to both IT and operations as needed, so that they can work in concert—as can be seen in this book (and already within this chapter), cyber security is an end-to-end problem that requires an end-to-end solution.
- *It is the same as "regular" cyber security*. This is another common misperception that can sometimes divide IT and plant operations' groups within an organization. "You have an Ethernet network; therefore, my UltraBrand Turbo-charged Firewall with this state-of-the-art unified threat management system will work just as well in the ICS as it does in the enterprise! After all, the vendor said it supported SCADA protocols, and all SCADA protocols are the same!" One thing that will become abundantly clear as you read this book is that industrial and business networks are different, and require different security measures to adequately protect them.

ASSUMPTIONS MADE IN THIS BOOK

The security practices recommended within this book aim for a very high standard, and in fact go above and beyond what is recommended by many government and regulatory groups. So which practices are really necessary, and which are excessive? It depends upon the nature of the industrial system being protected and the level of risk mitigation desired. What are the consequences of a cyber-attack? The production of energy is much more important in modern society than the production of a Frisbee (unless you happen to be a professional Ultimate Frisbee champion!). The proper manufacture and distribution of electricity can directly impact our personal safety by providing heat in winter or by powering our irrigation pumps during a drought. The proper manufacture and distribution of chemicals can mean the difference between the availability of flu vaccines and pharmaceuticals and a direct health risk to the population. Most ICSs are by their nature important regardless of an ICS's classification, and any risk to their reliability holds industrial-scale consequences. These consequences can be localized to a particular manufacturing unit, or spread to larger regional and national levels. While not all manufacturing systems hold life-and-death consequences, it does not mean that they are not potential targets for a cyber-attack. What are the chances that an extremely sophisticated, targeted attack will actually occur? The likelihood of an incident diminishes as the sophistication of the attack—and its consequences—grow, as shown in Figure 2.14. By implementing security practices to address these uncommon and unlikely attacks,

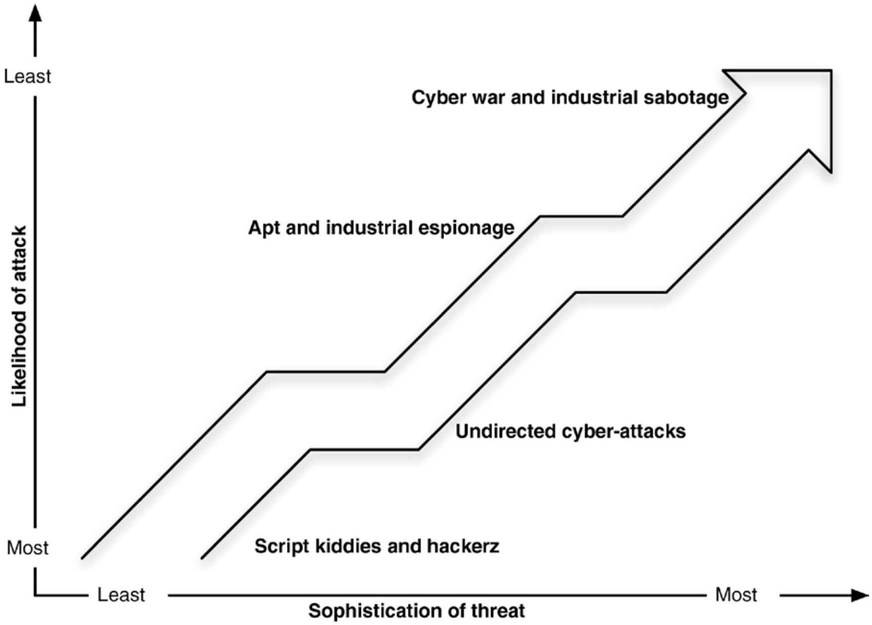

Least
Cyber war and industrial sabotage
Apt and industrial espionage
Likelihood of attack
Undirected cyber-attacks
Most
Script kiddies and hackerz
Least
Most
Sophistication of threat

FIGURE 2.14 Likelihood versus consequence of a targeted cyber-attack.

there is a greater possibility of avoiding the devastating consequences that correspond to them.

The goal of this book is to secure any industrial network. It focuses on critical infrastructure in particular, and will reference various standards, recommendations, and directives as appropriate. It is important to understand these directives regardless of the nature of the control system that needs to be secured, especially NERC CIP, Chemical Facility Anti-Terrorism Standards (CFATS), Federal Information Security Management Act (FISMA), ISA, and the control system security recommendations of the National Institute of Standards and Technology (NIST). Each has its own strengths and weaknesses, but all provide a good baseline of best practices for industrial network security. References are given when specific standards, best practices, and guidance are discussed. It is however, difficult to devote a great deal of dedicated text to these documents due to the fact that they are in a constant state of change. The industrial networks that control critical infrastructures demand the strongest controls and regulations around security and reliability, and accordingly there are numerous organizations helping to achieve just that. The Critical Infrastructure Protection Act of 2001 and HSPD-7 define what they are, while others—such as NERC CIP, NRC, CFATS, and various publications of NIST—help explain what to do.

SUMMARY

Understanding industrial network security first requires a basic understanding of the terminology used, the basics of industrial network architectures and operations, some relevant cyber security practices, the differences between industrial networks and business networks, and why industrial cyber security is important. By evaluating an industrial network, identifying and isolating its systems into functional groups or “zones,” and applying a structured methodology of defense-in-depth and strong access control, the security of these unique and specialized networks will be greatly improved. The remainder of this book will go into further detail on how industrial control systems operate, how they can be exploited, and how they can be protected.

ENDNOTES

1. Eric D. Knapp and Raj Samani, “Applied Cyber Security and the Smart Grid,” Elsevier, 2013.
2. North American Electric Corporation, Standard CIP–002–4, Cyber Security, Critical Cyber Asset Identification, North American Electric Corporation (NERC), Princeton, NJ, approved January 24, 2011.
3. North American Electric Corporation, Standard CIP–002–5.1, Cyber Security, Critical Cyber Asset Identification, North American Electric Corporation (NERC), Princeton, NJ, approved January 24, 2011.

4. Purdue Research Foundation (Theodore J. Williams, Editor); A Reference Model For Computer Integrated Manufacturing (CIM), A Description from the Viewpoint of Industrial Automation; Instrument Society of America, North Carolina, 1989.
5. North American Electric Corporation, Standard CIP–002–4, Cyber Security, Critical Cyber Asset Identification, North American Electric Corporation (NERC), Princeton, NJ, approved January 24, 2011.
6. Department of Homeland Security, Homeland security presidential directive 7: critical infrastructure identification, prioritization, and protection. <http://www.dhs.gov/xabout/laws/gc_1214597989952.shtm>, September, 2008 (cited: November 1, 2010).
7. U.S. Nuclear Regulatory Commission, The NRC: who we are and what we do. <http://www.nrc.gov/about-nrc.html> (cited: November 1, 2010).
8. Department of Homeland Security, Homeland security presidential directive/HSPD-7. Roles and responsibilities of sector-specific federal agencies (18)(d). <http://www.dhs.gov/xabout/laws/gc_1214597989952.shtm>, September 2008 (cited: November 1, 2010).
9. J. Arlen, SCADA and ICS for security experts: how to avoid cyberdouchery. in: Proc. 2010 BlackHat Technical Conference, July 2010.
10. U.S. Nuclear Regulatory Commission, Regulatory Guide 5.71 (New Regulatory Guide) Cyber Security Programs for Nuclear Facilities, U.S. Nuclear Regulatory Commission, Washington, DC, January 2010.