CHAPTER

Standards and Regulations 13

INFORMATION IN THIS CHAPTER

- Common Cyber Security Standards and Regulations
- ISA/IEC-62443
- Mapping Industrial Network Security to Compliance
- Mapping Compliance Controls to Network Security Functions
- Industry Best Practices for Conducting ICS Assessments
- Common Criteria and FIPS Standards

There are many cyber security standards, guidelines, and regulations imposed by governments and industry, which provide everything from "best practices" to hard requirements that are enforced through penalties and fines. Many of these standards are general information security documents; however, the number of industry-related documents focused on industrial control systems (ICSs) is growing. In the United States, common standards include the North American Electric Reliability Corporation's (NERC's) Critical Infrastructure Protection (CIP) Reliability Standards, the US Department of Homeland Security's (DHS) Chemical Facility Anti-Terrorism Standards (CFATS), the Regulated Security of Nuclear Facilities by the US Nuclear Regulatory Commission (NRC), and general ICS security recommendations published by the National Institute of Standards and Technology (NIST) in Special Publication 800-82. In Europe, standards and guidelines include the EU M/490 and the SGCG, which provide guidance for modern power, and the many publications of the European Union Agency for Network and Information Security (ENISA). Global standards include the ISO/IEC 27000 series of standards, of which ISO-27002:2013 "Code of practice for information security controls" is widely adopted.

Arguably the standard most relevant to industrial security is ISA 62443 (formerly ISA 99), which is the product of the International Society of Automation. ISA 62443 is concerned with the security of industrial automation and control systems, and is applicable to any organization or industry that uses these systems. ISA 62443 also aligns with international standard IEC 62443 and is under revision and restructuring for acceptance by the International Organization for Standardization (ISO) as ISO 62443.

Regardless of which standard you are working with, it is important to remember that standards are designed for a large and sometimes diverse audience, and so caution should be taken when applying them to an industrial architecture. These guidelines will make recommendations or requirements for specific cyber security controls, which have been vetted for general use by the target audience of the standard. However, even

when the target audience is suppliers, integrators, and end-users of ICS—as is the case with ISA 62443—there is no way for a standard to address the intricacies and nuances of an individual company or facility. No two networks are identical—even the same process within the same company will have subtle differences from site-to-site due to commissioning dates, system updates/migrations, and general lifecycle support. Therefore, each recommendation should be given careful consideration taking into account the specifics of your own unique industrial network environment.

This chapter attempts to map specific controls referenced in common standards to the relevant topics and discussions that are covered in this book (see Table 13.1). Please note that in many instances, policies and procedures may be the right answer; however, these are not covered in any detail in this book. You may realize, having made it to Chapter 13 that this book focuses largely on technology. This is not to suggest that people and process are less important to technology; only to explain that there are many additional security controls to consider beyond what is covered here. On a similar note, we will not attempt to focus on any one standard in detail within this book, because efforts to maintain compliance with just one of these regulations can be challenging and complex enough to fill entire books. Because of slight variations in terminology and methodology, complying with multiple standards can be a nightmare. However, it can often be valuable for someone who is attempting to follow a particular standard to utilize both the normative and informative text of other standards to gain additional insight and understanding that may be absent from the original document. "Crosswalks" between standards can be a valuable asset in mapping between the various standards and their particular requirements.

There are also standards and regulations that do not apply to industrial networks at all, but rather to the products that might be utilized by an industrial network operator to help secure (see Chapter 9, "Establishing Zones and Conduits") and monitor (see Chapter 12, "Security Monitoring of Industrial Control Systems") the network. Among these are the international Common Criteria standards, and various Federal Information Processing Standards (FIPS) including the FIPS 140-2 Security Requirements for Cryptographic Modules.

COMMON STANDARDS AND REGULATIONS

As mentioned in Chapter 2, "About Industrial Networks," industrial networks are of interest to several national and international regulatory and standards organizations. In the United States and Canada, NERC is well known because of the NERC CIP reliability standards, which heavily regulate security within the North American bulk electric system. NERC operates independently under the umbrella of the Federal Energy Regulatory Commission (FERC), which regulates interstate transmission of natural gas, oil, and electricity. FERC also reviews proposals to build liquefied natural gas (LNG) terminals, interstate natural gas pipelines, and licensing for hydropower projects. The Department of Energy (DoE) and DHS also produce several security recommendations and requirements, including the CFATS, the Federal Information Security Management Act (FISMA), and Homeland Security Presidential Directive

Seven, which all refer back to several special publications of the NIST, particularly SP 800-53 "Recommended Security Controls for Federal Information Systems and Organizations" and SP 800-82 "Guide to Industrial Control Systems (ICS) Security." The International Society of Automation's standard for the Security for Industrial Automation and Control Systems (ISA 62443), provide security recommendations that are applicable to industrial control networks. ISO also has published the ISO-27033 standard for network security, and is considering the release of industry-specific standard ISO-27013 for manufacturing systems.

NERC CIP

It is hard to discuss Critical Infrastructure security without referring to the NERC CIP reliability standards, which has gained wide notoriety due to its heavy penalties for non-compliance. Although NERC CIP standards are only enforceable within North American bulk electric systems, the standards represented are technically sound and in alignment with other standards, and are presented in the spirit of improving the security and reliability of the electric industry.[1] Furthermore, the critical infrastructures of the electric utilities—specifically the distributed control systems responsible for the generation of electricity and the stations, substations, and control facilities used for transmission of electricity—utilize common industrial network assets and protocols, making the standards relevant to a wider base of industrial network operators.

CFATS

The Risk-Based Performance Standards (RBPS) for the CFATS outline various controls for securing the cyber systems of chemical facilities. Specifically, RBPS Metric 8 ("Cyber") outlines controls for (1) security policy, (2) access control, (3) personnel security, (4) awareness and training, (5) monitoring and incident response, (6) disaster recovery and business continuity, (7) system development and acquisition, (8) configuration management, and (9) audits.

Controls of particular interest are Cyber Metric 8.2.1, which requires that system boundaries are identified and secured using perimeter controls, which supports the zone-based security model. Metric 8.2 includes perimeter defense, access control (including password management), the limiting of external connections, and "least-privilege" access rules.[2]

Metric 8.3 (Personnel Security) also requires that specific user access controls be established, primarily around the separation of duties, and the enforcement thereof by using unique user accounts, access control lists, and other measures.[3]

Metric 8.5 covers the specific security measures for the monitoring of asset security (primarily patch management and anti-malware), network activity, log collection and alerts, and incident response, whereas Metric 8.8 covers the ongoing assessment of the architecture, assets, and configurations to ensure that security controls remain effective and in compliance.[4]

Of particular note are RBPS 6.10 (Cyber Security for Potentially Dangerous Chemicals), RBPS 7 (Sabotage), RBPS 14 (Specific Threats, Vulnerabilities, and Risks), and RBPS 15 (Reporting)—all of which include cyber security controls outside of the

RBPS 8 recommendations for cyber security. RBPS 6.10 implicates ordering and shipping systems as specific targets for attack that should be protected according to RBPS 8.[5] RBPS 7 indicates that cyber systems are targets for sabotage and that the controls implemented "deter, detect, delay, and respond" to sabotage.[6] RBPS 14 requires that measures be in place to address specific threats, vulnerabilities, and risks, inferring a strong security and vulnerability assessment (SVA) plan,[7] whereas RBPS 15 defines the requirements for the proper notification of incidents when they do occur.[8]

ISO/IEC 27002

The ISO/IEC 27002:2013 Standard is part of the ISO/IEC 27000 series of international standards published by the ISO, the International Electrotechnical Commission (IEC), and the American National Standards Institute (ANSI). Figure 13.1 illustrates the organization of the ISO 27000 series. ISO 27002 was previously published as ISO 17799 and later renamed, outlines hundreds of potential security controls that may be implemented according to the guidance outlined in ISO 27001. Although ISO/IEC 27002 provides less guidance for the specific protection of industrial automation and control, it is useful in that it maps directly to additional national security standards in Australia and New Zealand, Brazil, Chile, Czech Republic, Denmark, Estonia, Japan, Lithuania, the Netherlands, Poland, Peru, South Africa, Spain, Sweden, Turkey, United Kingdom, Uruguay, Russia, and China.[9]

As with NERC CIP and CFATS, ISO/IEC 27002 focuses on risk assessment and security policies in addition to purely technical security controls. The 2013 revision includes 114 security controls that are discussed including asset management and configuration management controls, separation and security controls for network communications, specific host security controls regarding access control, and anti-malware protection. Of particular interest is a group of controls around security incident management—the first of the standards discussed in this book to specifically mention the anticipation of a security breach using anomaly detection. Specifically, ISO/IEC mentions "malfunctions or other anomalous system behavior may be an indicator of a security attack or actual security breach."[11]

In 2013, ISO/IEC released the energy-sector specific technical report TR27019:2013. This document expands on the requirements of NERC CIP by including distribution of electric power, as well as storage and distribution of gas and heat. The report includes 42 sector-specific additions and recommendations outside the current content of ISO/IEC 27002, including security controls for (potentially insecure) legacy systems, data communications, malware protection, and patch management for industrial systems.

NRC REGULATION 5.71

NRC Regulation 5.71 (RG 5.71) published in 2010 provides security recommendations for complying with Title 10 of the Code of Federal Regulations (CFR) 73.54. It consists of the general requirements of cyber security, including specific requirements for planning, establishing, and implementing a cyber-security program. Specific to RG 5.71 is the use of a five-zone network separation model, with one-way

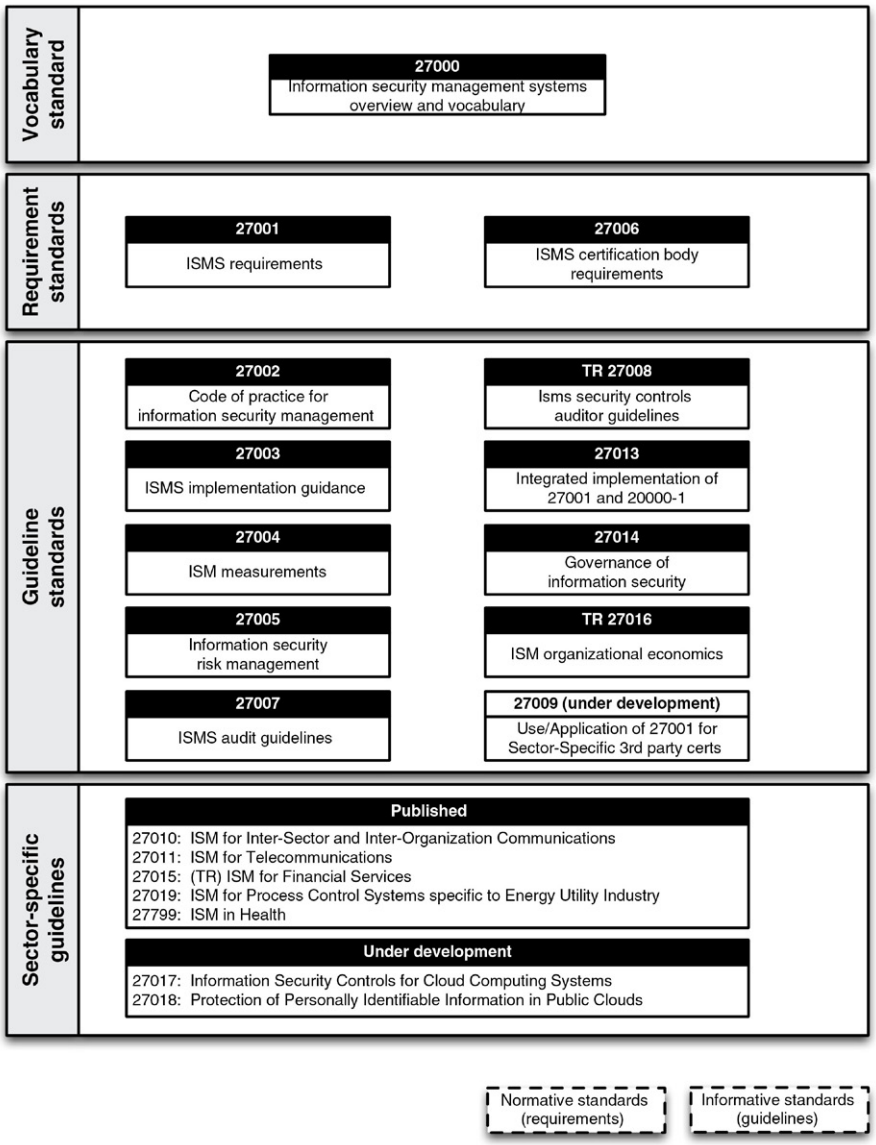

FIGURE 13.1 ISO 27000 organizational structure.[10]

communications being required between levels 4-3 and 3-2 (the most critical zones of the five labeled 4-0). One-way communication gateways, such as data diodes, allow outbound communications while preventing any return communications, promising an ideal security measure for the transmission of information from a secure zone to an outside supervisory system.

Although many of the recommendations in RG 5.71 are general in nature, RG 5.71 also includes three appendices, which provide a well-defined security plan template (Appendix A), technical security controls (Appendix B), and operational and management controls (Appendix C) for each recommendation.[12]

NIST SP 800-82

The National Institute of Standards and Technology published in May 2013 the latest revision to the "Guide to Industrial Control Systems (ICS) Security," which includes recommendations for Security, Management, Operational, and Technical controls in order to improve control system security. Revision 2 of this publication is currently in draft form (public comment period ended July 18, 2014) and comprises mainly recommendations, not hard regulations subject to compliance and enforcement. The controls presented are comprehensive and map well to additional NIST recommendations, such as those provided in Special Publication (SP) 800-53 ("Recommended Security Controls for Federal Information Systems and Organizations") and SP 800-92 ("Guide to Computer Security Log Management").[13]

ISA/IEC-62443

ISA 62443 is actually a series of standards, organized into four groups that address a broad range of topics necessary for the implementation of a secure Industrial Automation and Control System (IACS). The standard, which originated as ISA 99 when developed by the Standards and Practices Committee 99 (SP99), is now being aligned with IEC 62443. At the time of this writing, several of the documents produced under ISA 62443 have been published and adopted by IEC, while others remain in various stages of genesis. Due to timing, there is no guarantee that what is referenced here within this book will fully align with what is eventually published, so as always it is a good idea to reference the documents directly via ISA.org. The document number for each identifies the standard (62443), the Group Number, and the Document Number (e.g. ISA 62443-1-1 is document number "1," belonging to group "1" of the ISA 62443 standard). Figure 13.2 illustrates the organizational structure of the ISA 62443 series.

ISA 62443 GROUP 1: "GENERAL"

ISA 62443 Group 1 (ISA 62443-1-x) focuses on the standardization of terminology and consistency of references, metrics, and models, with the goal of establishing a baseline of the fundamentals that are then referenced within the other groups. At this time, there are four documents actively being developed, including a master glossary (62443-1-2) and definitions of an IACS security lifecycle (62443-1-4). Of particular interest is 62443-1-3, which defines conformance metrics that are extremely useful in quantifying compliance to IACS security practices. These metrics are also extremely valuable to cyber security information analytics platforms, exception reporting, and other useful security monitoring tools (see Chapter 12, "Security Monitoring of Industrial Control Systems").

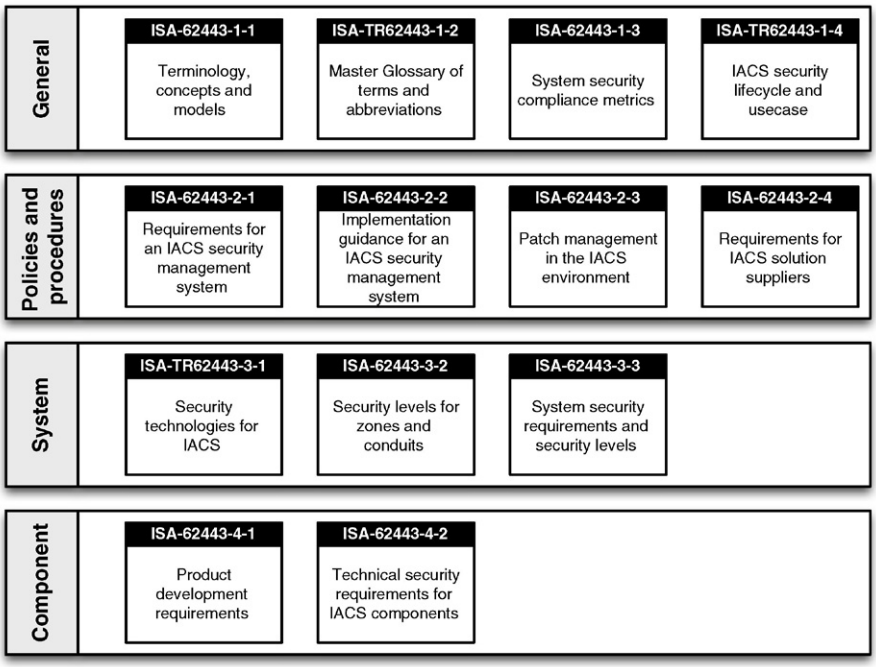

FIGURE 13.2 ISA 62443 organizational structure.[14]

ISA 62443 GROUP 2: "POLICIES AND PROCEDURES"

ISA 612443 Group 2 (ISA 62443-2-x) focuses on the necessary policies and procedures for the creation of an effective IACS security program. Group 2 includes 62443-2-1, which was one of the first standards published in the series, and details the requirements necessary for an IACS security management system. 62443-2-3 addresses patch management within industrial architectures (see Chapter 8, "Risk and Vulnerability Assessments"). 62443-2-4 has been adapted from guideline document "Process Control Domain Security Requirements for Vendors" originally developed by the Process Automation Users' Association (WIB) in Europe, and provides requirements for the certification of IACS suppliers.

ISA 62443 GROUP 3: "SYSTEM"

ISA 62443 Group 3 (ISA 62443-3-x) focuses on cyber security technologies, and includes documents covering available technologies, assessment and design methodologies, and security requirements and assurance levels. 62443-3 is where information and guidance on network zones and conduits will be found (along with reference models defined in 62443-1-1), as well as ISA's methodologies for risk assessments (these topics are also covered in Chapter 8, "Risk and Vulnerability Assessments," Chapter 9, "Establishing Zones and Conduits," and Chapter 10, "Implementing

Table 13.1 ISA 62443 Security Levels[15]

Security Level	Description
1	Prevent the unauthorized disclosure of information via eavesdropping or casual exposure
2	Prevent the unauthorized disclosure of information to an entity actively searching for it using simple means with low resources, generic skills and low motivation
3	Prevent the unauthorized disclosure of information to an entity actively searching for it using sophisticated means with moderate resources, IACS specific skills and moderate motivation
4	Prevent the unauthorized disclosure of information to an entity actively searching for it using sophisticated means with extended resources, IACS specific skills and high motivation

Security and Access Controls"). 62443-3-3 represents the security controls catalog applicable to IACS, in much the same manner as ISO 27002 "Security Techniques - Code of Practice for Information Security Management" and NIST 800-53 "Security and Privacy Controls for Federal Information Systems and Organizations." This document is divided into seven Foundation Requirements (FR) each containing multiple System Requirements (SR). Each SR then contains zero or more Requirement Enhancements (RE) where the level of security required is determine by the security level as described in Table 13.1.

ISA 62443 GROUP 4: "COMPONENT"

ISA 62443 Group 4 (ISA 62443-4-x) focuses on the secure development of components, and includes detailed requirements around establishing a Secure Development Lifecycle (SDLC) for IACS components. This includes guidance for component design, planning, code development and review, vulnerability assessments, and component level testing. 62443-4 supports the test and validation of component "robustness" to ensure that components used within an IACS are not unduly vulnerable to common network aberrations, anomalies, and excesses. 62443-4 aligns with the ISA Security Compliance Institute's (ISCI) ISASecure program, which provides three different levels of security certification aligned with the standards defined by 62443-4. This includes supplier product development for ICS systems (Security Development Lifecycle Assurance), embedded devices (Embedded Device Security Assurance), and systems (System Security Assurance). Device certification includes extensive robustness testing using ISCI-validated test tools including the Wurldtech (a GE company) Achilles Test Platform, Codenomicon's Defensics X test platform, and FFRI's Raven for ICS test platform. The result from the testing and certifications defined by 62443-4 is the establishment of a particular "capability" Security Level as described in Chapter 9, "Establishing Zones and Conduits" necessary to align the capabilities of ICS components with the design "target" established earlier in the automation project lifecycle.

MAPPING INDUSTRIAL NETWORK SECURITY TO COMPLIANCE

Again, there are many security regulations, guidelines, and recommendations that are published globally. Many are applicable to industrial networks; some are enforced, some not; some are regional; some are applicable to all industrial networks, while some (such as NERC CIP) apply to specific industries. Although most standards and regulations focus on a variety of general security measures (including physical security, security policy development and planning, training, and awareness), each has specific controls and measures for cyber security.

TIP

Many enforced compliance regulations (e.g. NERC CIP) require that "**compensating controls**" be used where a requirement cannot be feasibly met. Using additional compliance standards as a guide, alternate "compensating controls" may be identified. Therefore, even if the compliance standard is not applicable to a particular organization, the recommendations made within may prove useful.

These cyber security measures often overlap, although there are differences (both subtle and strong) among them. Efforts to normalize all the available controls to a common "compliance taxonomy" are being led by organizations, such as the Unified Compliance Framework (UCF), which has currently mapped close to 500 Authority Documents to a common framework consisting of thousands of individual controls.[16] The advantages of a common mapping are significant and include the following:

- Facilitating compliance efforts for organizations that are responsible for multiple sets of compliance controls. For example, a nuclear energy facility that must track industrial regulations, such as NRC Title 10 CFR 73.54, NRC RG 5.71, and **NEI** 08/09 requirements, as well as business regulations, such as Sarbanes-Oxley (SOX). Understanding which specific controls are common among all regulations prevents the duplication of efforts and can significantly reduce the costs of collecting, maintaining, storing, and documenting the information necessary for compliance.
- Facilitating the implementation of specific security controls by providing a comprehensive list of controls that must be implemented across all relevant standards and regulations.

This Chapter begins to map the security and compliance requirements for this purpose; however, owing to the extensive nature of most regulations, as well as the changing nature of specific compliance control documents, only a select sample of common controls has been included in this text.

INDUSTRY BEST PRACTICES FOR CONDUCTING ICS ASSESSMENTS

There are several documents published that discuss various methodologies for testing and assessing IT architectures. This number is greatly reduced when an attempt is made to identify documents that understand the unique nature of industrial networks,

Table 13.2 Industry Best Practices for Conducting ICS Assessments

Publishing Organization	Description
American Petroleum Institute / National Petrochemicals and Refiners Association (USA)	Security Vulnerability Assessment Methodology for the Petroleum and Petrochemicals Industries
Centre for the Protection of National Infrastructure (UK)	Cyber Security Assessments of Industrial Control Systems – A Good Practice Guide
Department of Homeland Security (USA)	Can be used to test ability to exploit vulnerabilities (Ethical Hacking)
Institute for Security and Open Methodologies	Open-Source Security Testing Methodology Manual
National Security Agency (NSA)	A Framework for Assessing and Improving the Security Posture of Industrial Control Systems (ICS)

and offer any guidance in safely, accurately and reliably performing these assessments. Table 13.2 provides a listing of most of the documents published on industrial security assessments.

DEPARTMENT OF HOMELAND SECURITY (USA) / CENTRE FOR PROTECTION OF NATIONAL INFRASTRUCTURE (UK)

The US Department of Homeland Security co-authored a guidance document in November 2010,[17] which the UK Centre for the Protection of National Infrastructure (CPNI) also published in April 2011[18] as a "Good Practice Guide." This guideline is comprehensive in content, and provides a well-documented assessment methodology or process flow chart for the testing process. The coverage of the testing process is extensive, and can form the foundation for any organization's internal methodology.

The guide discusses the uniqueness associated with industrial networks, and addresses the differences between assessing industrial environments and traditional IT architectures. In particular, it describes the differences between an "assessment" and a "penetration test" and how the goals desired from a particular exercise should be used to drive the overall process. The guide also provides a list of alternate methodologies that can be used to address specific requirements or constraints that may exist, including

- Lab assessments
- Component testing
- Functionality review
- Configuration review
- Risk assessments.

NATIONAL SECURITY AGENCY (USA)

The National Security Agency (NSA) published their framework in August 2010.[19] As the case with many of the documents, this framework is broad in nature and provides a high-level approach to conducting security assessments specifically for industrial systems. This document provides guidance that can be very helpful in assisting with risk assessments for ICS by helping assess the threats and understanding the resulting impacts or consequences.

The framework provides valuable information on the system characterization activity defined in the text as a "Network Connectivity Assessment." This is an important first step in understanding the complete system under consideration (SuC), and can be applied to any methodology as an early activity. The document also provides information on loss assessments and how to calculate metrics that help to identify important services within the architecture and consequences to the overall system operation should these services fail to perform as designed.

This framework provides guidance of assessment of threats by first identifying the roles and responsibilities of authorized users. The potential attack vectors that target these users is introduced along with the concept of "attack difficulty," which provides a more qualitative means of measuring the "likelihood" of a cyber-event occurring. This framework also stands out from others reviewed in that it provides steps on prioritization of the defense efforts in order to address weaknesses discovered during the assessment process.

AMERICAN PETROLEUM INSTITUTE (USA) / NATIONAL PETROCHEMICAL AND REFINERS ASSOCIATION (USA)

The American Petroleum Institute (API) and the National Petrochemical and Refiners Association (NPRA), both from the USA, were among the earliest publishers of security guidance material releasing their document in May 2003. The second edition of this document was released in October 2004.[20] This document does not contain any specific reference to industrial systems, but rather provides the most comprehensive approach in terms of a complete security analysis called a security vulnerability assessment (SVA). This document is industry-specific, but the examples provided and the associated process applies to a broad range of process and industrial sectors. It discusses the concepts of an SVA in terms of risk including the concept of "asset attractiveness" that offers a different approach to the underlying motivation that a potential attacker may have for a given target. This factor is then combined with the other common risk components (threat, vulnerability, consequences) to provide a form of risk screening that can be used to understand how risk differs from industry to industry.

Sample forms and checklists are part of the methodology, which have not been included in any of the other documents reviewed. Several real-world assessments are provided, covering petroleum refining, petroleum pipeline, and transportation and distribution systems for truck and rail.

INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES (SPAIN)

The Institute for Security and Open Methodologies is an open community and nonprofit organization that first published version 1.0 of the Open-Source Security Testing Methodology Manual in January 2001. The current version 3.0 was released in 2010.[21] The OSSTMM is generic in nature, and does not include any specific reference to industrial networks. The terminology used in the methodology is inconsistent with other ICS-related documents. So why is this methodology included?

This document provides valuable reference information that may be useful as a methodology is customized to a particular organization's unique needs. The document provides assistance in utilizing "quantitative" methods and metrics of assessing security over the more traditional "qualitative" approach. One area that is addressed within the methodology that is not covered in the other documents focuses on "human security testing," and the processes that can be used to assess the involvement of operational personnel within the overall assessment framework extending beyond simple social engineering measures. The methodology provides a valuable discussion on analyzing trust and using this to identify and correct security weaknesses.

The OSSTMM provides an extensive section on compliance, including not only standards-based requirements, but also a list of countries and legislative requirements within these countries.

COMMON CRITERIA AND FIPS STANDARDS

Unlike other standards, Common Criteria and Federal Information Processing Standards (FIPS) aim to certify security *products*, rather than security *policies* and *processes*. The Common Criteria for Information Technology Security Evaluation ("Common Criteria" or "CC") is an international framework that is currently recognized by Australia/New Zealand, Canada, France, Germany, Japan, the Netherlands, Spain, the United Kingdom, and the United States.[22] FIPS is defined by NIST in FIPS PUBs. Although there are several standards in FIPS, it is the FIPS 140-2 Standard that validates information encryption that is most relevant to information security products.

COMMON CRITERIA

Common Criteria's framework defines both functional and assurance requirements that security vendors can test against in order to validate the security of the product in question.[23] Certification by an authorized Common Criteria testing facility provides a high level of assurance that specific security controls have been appropriately specified and implemented into the product.

The evaluations required prior to certification are extensive and include

- Protection Profiles (PP)
- Security Target (ST)

- Security Functional Requirements (SFRs)
- Security Assurance Requirements (SARs)
- Evaluation Assurance Level (EAL).

The Security Target defines what is evaluated during the certification process, providing both the necessary guidance during evaluation as well as high-level indication of what has been evaluated after an evaluation is complete.[24]

The Security Targets are translated to the more specific Security Functional Requirements, which provide the detailed requirements against which the various STs are evaluated. The SFRs provide a normalized set of terms and requirements designed so that different STs for different products can be evaluated using common tests and controls, to provide an accurate comparison.

When common requirements are established for a particular product type or category, typically by a standards organization, they can be used to develop a common Protection Profile that is similar to an ST in that it provides a high-level indication of the assessment, but different in that the specific targets are predefined within the PP.[25] For example, there is a Common Criteria Protection Profile for Intrusion Detection and Prevention Systems that defines the specific STs that an intrusion detection system (IDS) or intrusion prevention system (IPS) must meet to earn certification.

Perhaps the most commonly identified CC metric is the Evaluation Assurance Level (EAL). EALs measure Development (ADV), Guidance Documents (AGD), Lifecycle Support (ALC), Security Target Evaluation (ASE), Tests (ATE), and Vulnerability Assessment (AVA).[26] There are seven total assurance levels, EAL 1 through EAL 7, each of which indicates a more extensive degree of evaluation against a more exhaustive set of requirements for each of these components. For example, to compare just one of the evaluation requirements (AVA-Vulnerability Assessment), CC EAL 1 provides a basic level of assurance using a limited security target, and a vulnerability assessment consisting only of a search for potential vulnerabilities in the public domain.[27] In contrast, EAL 3 requires a "vulnerability analysis … demonstrating resistance to penetration attackers with a basic attack potential,"[28] and EAL 4 requires a "vulnerability analysis … demonstrating resistance to penetration attackers with an Enhanced-Basic attack potential" (i.e. more sophisticated attack profiles for a more thorough vulnerability assurance level).[29] At the most extensive end of the certification assurance spectrum is EAL 7, which requires "complete independent confirmation of the developer test results, and an independent vulnerability analysis demonstrating resistance to penetration attackers with a high attack potential."[30]

It is important to understand that the EAL level does not measure the level of security of the product that is under evaluation, but rather measures the degree to which the product's security is tested. Therefore, a higher EAL does not necessarily indicate a more secure system. It is the specific STs being evaluated that indicate the functional requirements of the system. When comparing like systems that are tested against identical targets, the higher EAL indicates that those

targets were more thoroughly tested and evaluated, and therefore, the higher EAL provides additional confidence or assurance in the proper and secure function of the system.

FIPS 140-2

The Federal Information Processing Standards Publication (FIPS PUB) 140-2 establishes the requirements for the "cryptographic modules" that are used within a cyber asset or system. There are four qualitative levels of FIPS validation, Levels 1 through 4, which like Common Criteria's EALs intend to validate increasingly thorough assurance. With FIPS 140-2, this assurance is in the form of cryptographic integrity; basically, how resistant encrypted boundaries are to penetration.[31] FIPS 140-2 covers the implementation and use of Symmetric and Asymmetric Keys, the Secure Hash Standard, Random Number Generators, and Message Authentication.[32] The specific validation levels represent increasingly more stringent controls to prevent physical access to information with the encrypted boundary. For example, FIPS 140-2 Level 2 requires that data cannot be accessed physically, even through the removal of disk drives or direct access to system memory. Level 3 provides stronger physical controls to prevent access to and tampering, even through ventilation holes, whereas Level 4 even accommodates environmental failures to protect the encrypted data against recovery during or following a failure.[33]

CAUTION

FIPS 140-2 defines what are called security assurance "levels," numbered 1 to 4 with 1 represented the lowest level of security requirements and 4 the highest allowing appropriate solutions be deployed based on unique local requirements. These security levels are not the same as those defined by ISA 62443, and cannot be used interchangeably when working with the various standards.

SUMMARY

Understanding how regulatory standards and regulations can impact the security of a network or system will help at all stages of industrial network security planning and implementation. Specific compliance controls might dictate the use of certain products or services to improve security, and/or how to configure those security products.

The security products themselves are subject to regulation as well, of course. The Common Criteria standards provide a means for evaluating the function and assurance of a product in a manner designed to facilitate the comparison of similar products, whereas standards in FIPS, such as FIPS 140-2, can provide further validation of specific security functions (in this case, encryption) used by a product.

Table 13.3 Sample Mappings of Regulations and Guidelines to Cyber Security Controls

Example Requirements	Recommendations	Chapter to Reference
• Establish Electronic Security Perimeter (NERC CIP) • Establish System Boundaries (CFATS) • Establish Secure Conduit (ISA-62443) • Segregation of Networks (ISO/IEC 27002:2005) • Sensitive System Isolation (ISO/IEC 27002:2005) • Cyber Security Controls (CFATS) • Access Control Lists (CFATS) • Network Connection Control (ISO/IEC 27002:2005) • Network Routing Control (ISO/IEC 27002:2005) • Information Flow Enforcement (NRC) • Network Architecture Control / Firewall between Corporate Network and Control Network (NIST 800-82) • Security Control, Intrusion Detection and Prevention (NIST 800-82) • Network Access Control (NRC) • Information Flow Enforcement (NRC)	• Implement network segmentation at Layer 2 (VLANs), or Layer 3 (Subnets). If segmentation is not supported due to ICS requirements (e.g. multicast messaging), filter traffic at the switch to control traffic. • Add network security to control traffic between segments. This can include: • NAC • ACLs • Firewalls • NGFW • IPS • Application Filters • UTM	• Chapter 5, "Industrial Network Design and Architecture" • Chapter 9, "Establishing Zones and Conduits" • Chapter 10, "Implementing Security Controls"
• Electronic Access Control (NERC CIP) • User Authentication for External Connections (ISO/IEC 27002:2005) • Password Requirements (NRC) • Password management (CFATS) • Unique Accounts (CFATS) • User Registrations (ISO/IEC 27002:2005) • Access Enforcement (NRC) • User Identification and Authentication (NRC)	• Require authentication to access all privileged network zones and all data contained therein. • Maintain least-privilege and separation of duties on all user accounts • Maintain strong password management on all user accounts • Monitor all user activity for indicators of inappropriate data access. • Implement Identity Access Management (IAM) tools to manage user accounts and ensure strong authentication and authorization practices.	• Chapter 10, "Implementing Security Controls" • Chapter 12, "Security Monitoring of Industrial Control Systems"

(*Continued*)

Table 13.3 Sample Mappings of Regulations and Guidelines to Cyber Security Controls (*cont.*)

Example Requirements	Recommendations	Chapter to Reference
• Monitoring Electronic Access (NERC CIP) • Network Monitoring (CFATS)	• Monitor network flows to validate network segmentation and ensure that network configurations and implemented security controls are functioning as intended. This can include the use of: • Network Management (NMS) • Network Behavior Anomaly Detection (NBAD) • Log Management System (LMS) • Security Information and Event Management system (SIEM)	• Chapter 11, "Exception, Anomaly and Threat Detection" • Chapter 12, "Security Monitoring of Industrial Control Systems"
• Denial of Service Protection (NRC)	• Ensure that proper zoning is in place and that industrial systems are not exposed to the Internet. • Implement anti-DoS technology in outer perimeters (e.g. between business networks and the Internet). • Validate critical network, security and ICS components are robust (i.e. test for resiliency during traffic anomalies and floods).	• Chapter 10, "Implementing Security Controls" • Chapter 8, "Risk and Vulnerability Assessments"
• Remote Diagnostic and Configuration Port Protection (ISO/IEC 27002:2005)	• Maintain a protected network zone for all external connectivity and remote communication, and control access into and out of this zone.	• Chapter 5, "Industrial Network Design and Architecture" • Chapter 9, "Establishing Zones and Conduits" • Chapter 10, "Implementing Security Controls"

Example Requirements	Recommendations	Chapter to Reference
• Change Control and Configuration Management (NERC CIP. NRC) • Change Management (ISO/IEC 27002:2005) • Changes to File System and Operating System Permissions (NRC)	• Host configuration monitoring using built-in Windows security audit tools and/or Linux *auditd* tool • Additional host cyber security controls for File Integrity Monitoring (FIM) and Configuration Management • Host cyber security controls to prevent file tampering or changes, including Host Intrusion Detection Systems (HIDS) and Application Whitelisting (AWL). • Monitor hosts for indications of file tampering or unauthorized changes. This can include the use of: • Log Management System (LMS) • Security Information and Event Management system (SIEM)	• Chapter 10, "Implementing Security Controls" • Chapter 12, "Security Monitoring of Industrial Control Systems"
• Ports and Services (NERC CIP) • Removal of Unnecessary Services and Programs (NRC) • Open and Insecure Protocol Restrictions (NRC)	• Monitor hosts for open ports and services using asset management or configuration management tools. • Monitor network and log behavior for indicators of unauthorized ports and services that may be in use, using SIEM and similar tools.	• Chapter 12, "Security Monitoring of Industrial Control Systems"
• Patch Management (NERC CIP) • Control of Technical Vulnerabilities (ISO/IEC 27002:2005) • Cyber Vulnerability Assessment (NERC CIP) • Vulnerability Scans and Assessments (NRC)	• Perhaps the most difficult challenge in industrial cyber security, patching is fundamental to maintaining a strong security posture. • The most important ingredient to good patch management is knowledge: keep informed of the latest vulnerabilities and threats, and keep your patch management procedure fluid enough to accommodate urgent patching requirements. • Automated solutions can ease this burden (e.g. using WSUS for Windows system and security patches).	• Chapter 8, "Risk and Vulnerability Assessments"

(*Continued*)

Table 13.3 Sample Mappings of Regulations and Guidelines to Cyber Security Controls (*cont.*)

Example Requirements	Recommendations	Chapter to Reference
• Cyber Asset Identification (CFATS)	• Implement access management either procedurally or through the use of asset management tools. • Implement security monitoring tools such as SIEM, preferably with integrated asset management capabilities.	• Chapter 8, "Risk and Vulnerability Assessments" • Chapter 11, "Exception, Anomaly and Threat Detection" • Chapter 12, "Security Monitoring of Industrial Control Systems"

• Malicious Software Prevention (NERC CIP)
• Cyber Security Controls (CFATS)
• Controls against Malicious Code (ISO/IEC 27002:2005)
• Host Intrusion Detection System (NRC)
• Malicious Code Detection (NIST 800-82)
• Anti-virus
• Malware Protection
	• To protect against malware, both host-based and network-based security controls should be used. Because malware changes often, multiple layers of defense are recommended, and all anti-malware efforts should be well-managed, and kept current with any necessary patches or updates.
	• Host cyber security controls including:
	  • Endpoint hardening to minimize the vulnerability of devices to malware
	  • Anti-virus, Application Whitelisting and/or HIDS to prevent the effectiveness of malware
	• Network
	• Network cyber security controls including:
	  • Segment the network to minimize the propagation or spread of malware if/when it occurs.
	  • Implement Network traffic inspection (DPI) using IPS to prevent known exploits and malware from traversing the network.
		• Chapter 5, "Industrial Network Design and Architecture"
		• Chapter 9, "Establishing Zones and Conduits"
		• Chapter 10, "Implementing Security Controls"

Example Requirements	Recommendations	Chapter to Reference
• Incident Reporting (CFATS, NERC CIP) • Audit Logging (ISO/IEC 27002:2005) • Reporting Information Security Events (ISO/IEC 27002:2005) • Collection of Evidence (ISO/IEC 27002:2005) • Records Retention and Handling (NRC)	• While incident reporting can be largely procedural, a good Log Management or SIEM solution can assist with the auditing of evidence and activities surrounding an incident, produce supporting documentation, and store the records (in this case, the event logs) in a secure, nonrepudiated manner.	• Chapter 12, "Security Monitoring of Industrial Control Systems"
• Monitoring Electronic Access (NERC CIP) • Security Status Monitoring (NERC CIP) • Network Monitoring (CFATS) • Monitoring System Use (ISO/IEC 27002:2005) • Security Alerts and Advisories (NRC) • Continuous Monitoring and Assessment (NRC)	• Again, a good Log Management or SIEM solution will collect data from the network in addition to security events, providing a continuous monitoring solution needed to support a variety of standards. Most solutions will include standard-specific report templates as well, further easing compliance efforts.	• Chapter 12, "Security Monitoring of Industrial Control Systems"

ENDNOTES

1. M. Asante, NERC, Harder questions on CIP compliance update: ask the expert, 2010 SCADA and Process Control Summit, The SANS Institute, March 29, 2010.
2. Department of Homeland Security, Risk-Based Performance Standards Guidance; Chemical Facility Anti-Terrorism Standards, May 2009.
3. Ibid.
4. Ibid.
5. Ibid.
6. Ibid.
7. Ibid.
8. Ibid.
9. International Standards Organization/International Electrotechnical Commission (ISO/IEC), About ISO. http://www.iso.org/iso/about.htm (cited: March 21, 2011).
10. "Information technology – Security techniques – Information security management systems – Overview and vocabulary," ISO/IEC 27000:2014, 3rd Edition, January 15, 2014.
11. International Standards Organization/International Electrotechnical Commission (ISO/IEC), International ISO/IEC Standard 27002:2005 (E), Information Technology—Security Techniques—Code of Practice for Information Security Management, first edition 2005-06-15.
12. U.S. Nuclear Regulatory Commission, Regulatory Guide 5.71 (New Regulatory Guide) Cyber Security Programs for Nuclear Facilities, January 2010.
13. K. Stouffer, J. Falco, K. Scarfone, National Institute of Standards and Technology, Special Publication 800-82 (Final Public Draft), Guide to Industrial Control Systems (ICS) Security, September 2008.
14. ISA99 Committee on Industrial Automation and Control Systems Security, <http://isa99.isa.org>, sited July 21, 2014.
15. "Security for industrial automation and control systems: System security requirements and security levels," ISA 62443-3-3:2013.
16. The Unified Compliance Framework, What is the UCF? <http://www.unifiedcompliance.com/what_is_ucf> (cited: March 21, 2011).
17. "Cyber Security Assessments of Industrial Control Systems," U.S. Dept. of Homeland Security, November 2010.
18. "Cyber Security Assessments of Industrial Control Systems – A Good Practice Guide," Centre for the Protection of National Infrastructure, April 2011.
19. "A Framework for Assessing and Improving the Security Posture of Industrial Control Systems (ICS)," National Security Agency, August 2010.
20. "Security Vulnerability Assessment Methodology for the Petroleum and Petrochemical Industries," API SVA-2004, American Petroleum Institute / National Petroleum Refiners Association, 2nd Edition, October 2004.
21. "Open-Source Security Testing Methodology Manual," Version 3.0, Institute for Security and Open Methodologies, 2010.
22. The Common Criteria Working Group, Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, Version 3.1, Revision 3 Final, July 2009.
23. Ibid.
24. Ibid.
25. Ibid.

26. The Common Criteria Working Group, Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components, Version 3.1, Revision 3 Final, July 2009.
27. Ibid.
28. Ibid.
29. Ibid.
30. Ibid.
31. National Institute of Standards and Technology, Information Technology Laboratory, Federal Information Processing Standards Publication 140-2, Security Requirements for Cryptographic Modules, May 25, 2001.
32. Ibid.
33. Ibid.