Chapter 1
Introduction and Preview

Alexander Kott, Carlos Aguayo Gonzalez, and Edward J.M. Colbert

The term Industrial Control System (ICS) refers to a variety of systems comprised of computers, electrical and mechanical devices, and manual processes overseen by humans; they perform automated or partially automated control of equipment in manufacturing and chemical plants, electric utilities, distribution and transportation systems and many other industries.

While strong concerns about security of ICSs, particularly in the context of critical national infrastructure, were expressed even in early 2000s (Lüders 2005; US Department of Energy 2002), it was not until the legendary 2010 Stuxnet episode (Langner 2011) that security of ICSs entered public and government discourse and acquired today's saliency (Executive Order 2013; Stouffer et al 2015).

This book takes a broad-ranging look at cyber security of ICS: from exploring types of components, layers, zones and sub-systems of ICS, to threats and attacks on ICS, to intrusion detection specific to ICS, to risk assessment and governance of ICS, to future of ICS.

Edward J.M. Colbert - Also ICF International, Inc.

A. Kott (✉) • E.J.M. Colbert
US Army Research Laboratory, Adelphi, MD, USA
e-mail: alexander.kott1.civ@mail.mil; edward.j.colbert2.civ@mail.mil

C. Aguayo Gonzalez
PFP Cybersecurity, Vienna, VA, USA

E.J.M. Colbert, A. Kott (eds.), *Cyber-security of SCADA and Other Industrial Control Systems*, Advances in Information Security 66,
DOI 10.1007/978-3-319-32125-7_1

In this introductory chapter we begin by exploring basic concepts and segments of the general class of Cyber-Physical Systems (CPSs), which include ICSs and SCADA[1] systems. This helps understand the differences between cyber security of ICSs and that of conventional IT systems. Then, we provide a preview of the entire book.

1.1 The Structure and Functions of an ICS

A key difference between ICSs and traditional Information Technology (IT) systems is that ICSs interact strongly with the physical environment. ICSs and all CPSs are cybersystems and are therefore vulnerable to cyber attacks. This connection with the physical world, however, presents unique challenges and opportunities.

CPSs integrate computational resources, communication capabilities, sensing, and actuation in effort to monitor and control physical processes. CPSs are found in critical infrastructure such as transportation networks, Unmanned Aerial Vehicle Systems (UASs), nuclear power generation, electric power distribution networks, water and gas distribution networks, and advanced communication systems.

In traditional critical infrastructure systems great efforts are committed to address concerns about safety and reliability, and to develop the appropriate techniques for fault detection, isolation, and recovery. In CPSs, however, the additional "cyber" element introduces specific vulnerabilities which are not directly addressed in traditional fault tolerance and reliable computing practices. Addressing the cyber element in CPS safety and reliability is of utmost importance, since the introduction of highly integrated CPS into critical infrastructures and emerging systems could lead to situations where cyber based attacks against CPSs could adversely affect widespread public safety (Cardenas 2008).

1.1.1 Key Segments of an ICS

In general, ICSs can be very complex systems. They can involve thousands of different components distributed across geographical regions and controlling complex processes at real-time. Most of the time, the large scale of these systems, as well as the diversity of devices and requirements, requires ICS systems to be segmented into multiple operational zones. Each operational zone has unique characteristics and requirements. In order to cope with the complexity, different models have been developed to represent ICS systems (IEC TS 62443-1-1 2009; NIST 2014). From a cyber security perspective, ICS systems can be broadly segmented into three different zones:

- Enterprise zone,
- Control zone, and
- Field zone.

[1] Supervisory Control and Data Acquisition (SCADA) systems are a sub-class of ICSs in which control is performed over multiple, distributed individual lower-level control systems (hence the word "supervisory"). See Chap. 2 for a more detailed discussion of the different types of ICSs.

Having this segmentation is extremely useful in determining relevant security controls. The three-zone model has been used (IEC TS 62443-1-1 2009; Knapp 2012), although different names are often used to refer to similar concepts. The general components and characteristics of each zone are shown in Fig. 1.1 and described below.

The Enterprise zone includes business networks and enterprise systems; it includes diverse endpoint devices that evolve rapidly and are upgraded continuously. This zone includes business networks, commonly based on the IP protocol and very often connected to external networks and the Internet. These networks are most of the time kept separate from the operational networks used in the other zones. The enterprise zone is very similar to traditional IT environments found outside the realm of ICSs. Therefore, many cybersecurity solutions from the IT world can be directly applied.

The Control zone includes the distributed control elements in SCADA systems. These zones include the control room environments. The Control zone shares a few similarities with the Enterprise zone, such as networks based on the IP protocol. The requirements of the Control zone, however, shift drastically to emphasize safety and reliability. The devices in this zone may not be updated as often and the networks may be subject to strict timing constraints. Therefore, few cybersecurity solutions from the IT world can be directly used in this zone.

The Field zone, also known as the plant, process, or operations zone, includes the devices and networks in charge of control and automation. The field zone is the one that hosts the CPSs. The devices in this zone often include single-purpose embedded

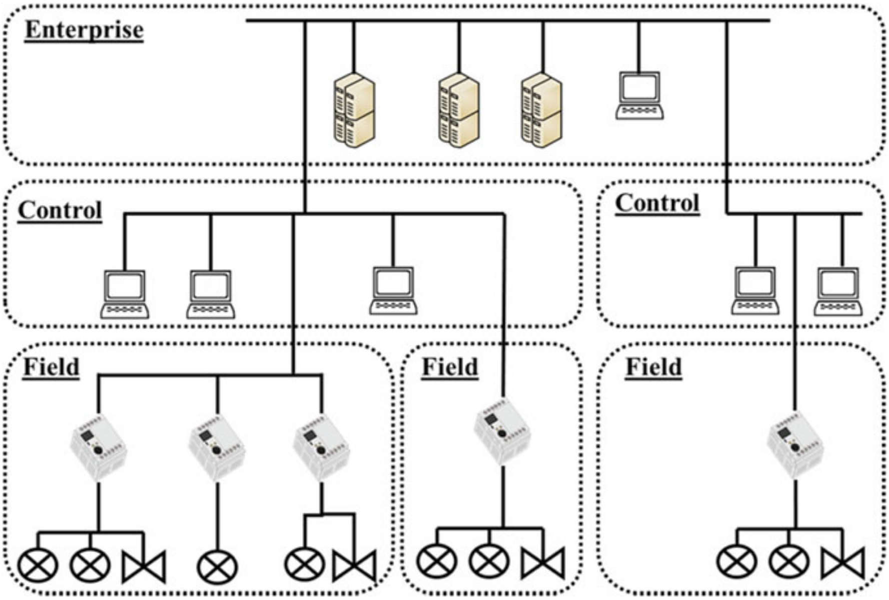

Fig. 1.1 ICS three-tiered security model

devices, such as Programmable Logic Controllers (PLCs), which have constrained computational resources. The communication networks in this zone are much more diverse and go beyond IP networks, employing a large variety of industrial protocols and physical interfaces. Devices and networks in the field zone are subject to strict safety, reliability, and timing requirements. Therefore, the cybersecurity solutions from the IT world rarely if ever apply.

This three-tiered model is admittedly oversimplified. However, it is very useful to differentiate the unique technical aspects that shape security requirements. Each zone has different security requirements and it is important to establish strong boundaries and abstractions between zones. The consequences of cyber attacks on the different zones are also very different.

A good example of different operational zones in ICSs is found in the modern electrical smart grid. At the same time it exemplifies how modern ICSs are very complex systems that often do not fit a general network models for cybersecurity. For instance, the smart grid is a sophisticated architecture of communication, control, monitoring, and automation with a goal of improving the way electricity is generated, distributed, and consumed. The smart grid is distributed across vast geographical regions and includes multiple zones, including multiple field zones, each one very complex in itself.

As shown in Fig. 1.2, the smart grid is separated into four major areas: generation, transmission, and distribution of energy, as well as the advanced metering at the end-user premises. Each one of the major areas is a vast and a very complex system on its own, with multiple field and control zones that need to interact with one another. The smart grid also highlights the complexity and diversity at the enterprise levels. The smart grid requires a variety of energy services and back-office services that while included in the enterprise zone, could be considered their own zone.

It can be argued that current cybersecurity approaches for the smart grid adequately protect higher zones (such as IT networks), since they share many commonalities with other enterprise level systems. The energy generation, transmission and distribution areas, however, rely heavily on CPSs and include vast distributed field zones made up of ICSs with dedicated and limited functionality. Protecting such complex systems from cyber attack is a daunting challenge which designers need to meet along with additional constraints, such as safety and reliability requirements.

1.1.2 Safety and Reliability in ICS

One of the main operational distinctions on the Field zone as compared with the Enterprise zone is the strict requirements for reliability and safety, especially for control of critical infrastructure. For example, Field devices in critical infrastructure are designed as safety-critical, fault-tolerant systems. These safety and reliability requirements have a profound impact in multiple aspects of ICSs, from design (e.g., redundant systems) to maintenance (e.g., upgrading and patches). Because of this, we give special attention to describing the specific requirements that arise as results of safety and reliability requirements in field devices and networks.

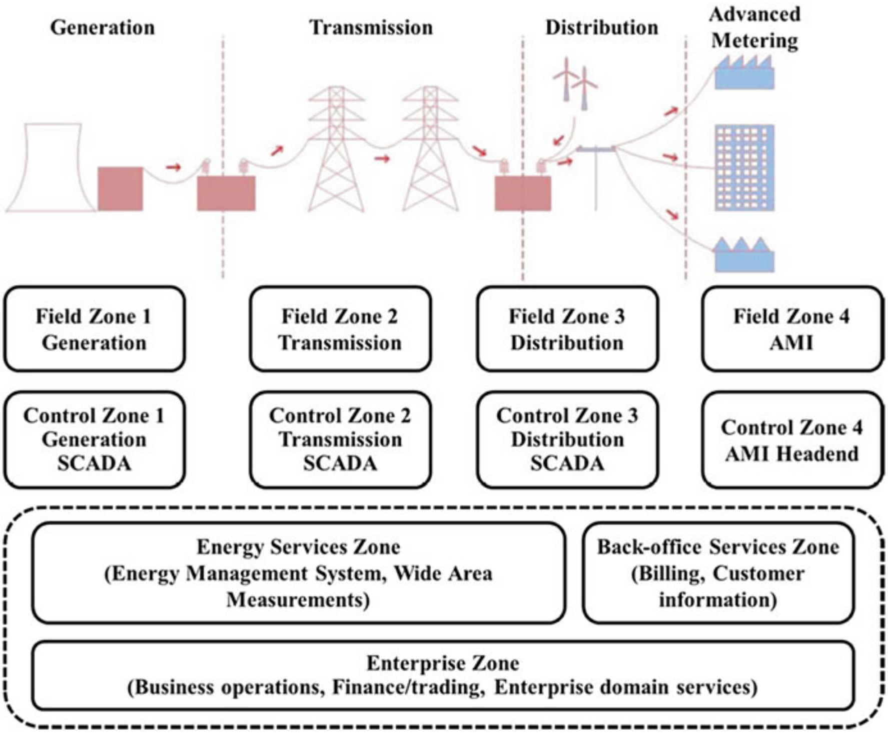
Generation
Transmission
Distribution
Advanced Metering
Field Zone 1 Generation
Field Zone 2 Transmission
Field Zone 3 Distribution
Field Zone 4 AMI
Control Zone 1 Generation SCADA
Control Zone 2 Transmission SCADA
Control Zone 3 Distribution SCADA
Control Zone 4 AMI Headend
Energy Services Zone (Energy Management System, Wide Area Measurements)
Back-office Services Zone (Billing, Customer information)
Enterprise Zone (Business operations, Finance/trading, Enterprise domain services)

Fig. 1.2 Operational zones example in the Smart Grid

Field systems in critical infrastructure are required to provide very high levels of availability, on-demand reliability, and in some cases safety under a wide range of operating conditions. Because of the potential consequences of a critical system's failure, these systems must reduce the likelihood of even low-probability fault events. Systems where the consequences of failure are high must be dependable systems, which have the ability to avoid service failures that are more frequent and more severe than is acceptable to the user(s) and also have the ability to deliver service that can be justifiably trusted. Dependable systems often use the following approaches to enhance the reliability and safety of the systems in the presence of faults:

- Fault avoidance—avoid faults by design, i.e., build the system correctly from the beginning
- Fault removal—reduce, by verification and testing the presence of faults
- Fault tolerance—provide correct function despite presence of faults

Fault tolerance is the only one active in the operational phase. Thus, for the fault tolerance techniques to work effectively, it is important to understand the types of faults the system may experience. Traditionally, fault tolerance methods and techniques have been used for two classes of faults/failures. The first is hardware faults that could be permanent or transient in nature. The second is software faults that become active when unusual inputs and state conditions occur. Both hardware and software fault tolerance techniques make use of redundancy to overcome the effects of faults.

Hardware fault tolerance methods use techniques like voting, masking, EDC codes, duplication and comparison to detect and correct the effects of faults. These techniques work for hardware faults because hardware faults are assumed to occur randomly, independently of one another. Software faults usually do not occur randomly or independently from one another, they occur when input/state conditions arise that trigger a software bug. As such, merely replication and redundancy do not work.

Software fault tolerance techniques often employ diversity and defense-in-depth techniques to detect and correct software faults at runtime. These include: diverse forms of the software running on different processors, N-version programming where different versions of the program are written by diverse programming teams, runtime monitors where a "safety monitor" checks the outputs for reasonableness or a property violation. In general, fault-tolerant systems relay on resilient designs and continuous state awareness or monitoring. In these systems, self-monitoring and self-testing features are prominent such as cyclic hardware testing, timing analysis to detect processes that hang, independent watchdog timers, hardwired shutdown in the case of failure, data integrity checks, and in case of failure, faulty messages and signals are used by application level error detection to enforce fail-safe operation.

Another important characteristic of dependable systems is that they are often real-time. A real-time system is characterized by its ongoing interaction with its environment, continuously accepting requests from the environment and continuously producing reactions. In real time systems, correctness or safeness of the reactive system is related to its behavior over time as it interacts with its environment. Thus, correctness of the result also depends on timeliness of delivery.

While hardware and software fault tolerant methods are sufficient for randomly occurring or design faults, they are not sufficient when the faults are malicious and intentional in nature—faults caused by cyber attacks. In the context of CPSs, true resiliency must consider what represents the proper operation of the process application in the face of many adverse conditions, including those attributable to threats from undesirable human interactions, such as those of malicious cyber actors. Cyber faults in CPSs fall into two classes.

- Non-malicious failures, introduced without malicious objectives
- Malicious failures or cyber-attacks, introduced during either system development with the intent to cause harm to the system during its use, or directly during use

While non-malicious faults and failures are mostly introduced by inadvertent mistakes and bad operator decisions, malicious failures or cyber-attacks are introduced by an intelligent human adversary or threat agent with the malicious objective to alter the functioning of the system. For instance, an adversary could launch an external attack in which the attacker intercepts messages, injects false data, or denies access to certain modules. While these actions can certainly disrupt the operation of the system, they can be detected and mitigated with current technologies, such as firewalls, encryption, and authentication. In other cases, an attacker could compromise and completely control some system components. In this scenario, the attacker could modify or drop critical messages, inject false reporting and monitoring information, generate false events, disable critical safety measures, coordinate attacks involving multiple components, and much more.

1.1.3 Security of ICS Field Network Components

The Field Zone in ICSs epitomizes the differences between traditional cybersecurity in IT systems and ICSs. Systems in the field zones, including the endpoints (such as controllers) and its networks (conduits), are often the ones with the most stringent requirements in terms of reliability and safety, and the most sensitivity to timing disruptions. They are often implemented with severe resources constraints, often relying on legacy platforms that are not updated or patched, and using proprietary communication protocols.

Current approaches are limited to monitoring the conduits (access networks) to the field zones that attempt to create protected "islands", but can still leave Field elements unprotected and unmonitored. Existing cyber security approaches typically cannot be applied to the field elements due to the limited computational capabilities of the field elements. Current approaches for protecting the Field zone from cyber attack are traditionally limited to physical security, while network security (e.g., intrusion prevention and intrusion detection) is often limited to the conduits, and end-point protection to a limited extent. In terms of endpoint protection for Field devices, current cyber security solutions do not meet the field requirements adequately. For instance, there is lack of adequate antivirus software for the embedded systems in CPSs, and monitoring techniques that rely in virtual machine hypervisors are difficult to deploy in resource-constrained, legacy embedded platforms common in field devices.

While the Field zone highlights the difficulty in protecting ICSs from cyber attacks, the challenges presented by the Field zone operational environment also impact the attacker's ability to achieve their malicious objectives without being detected or triggering safety events. In a way, the Field zone is the most difficult to attack, since attackers need to have intimate knowledge of the process and systems in order to achieve the malicious objectives without being discovered, and without triggering any of the safety and security mechanisms (Krotofil 2015).

The interaction with the physical world, therefore, presents unique opportunities to protect field systems. Researchers have explored measuring the physical process to validate that the cyber element has not been compromised. For instance, electricity theft detectors where data analytics software is used by the utility on the collected meter data to identify possible electricity theft situations and abnormal consumption trends. This approach leverages the information provided by physical sensors to detect potential cyber attacks (Nizar 2009).

1.2 Preview of this Book

Having introduced some key features, characteristics and challenges of ICSs, let us offer the reader a preview of this book. We (here "we" refers collectively to all co-authors of this book) begin the discussion of ICS security with the Chap. 2 by introducing the basic components of ICSs, their functions, variety, and ways in which they connect and interact to produce the intended effects. The scope of an ICS may vary enormously. It ranges from a single PLC controlling a motor, to an ICS controlling a utility company's power generation plant or an ICS that control a nation's power transmission system. ICS configurations also differ greatly. Such configurations may range from a single component to wide area networks spanning a whole continent with many thousands of ICS components. In spite of such diversity, the basic building blocks of an ICS can be assigned to only a few classes. These include for example PLCs, Remote Terminal Units, Communication Gateways, and a few others which we discuss in this chapter. Unlike an IT system, an ICS monitors or interacts with something physical in the real world, and therefore an ICS includes field devices. ICSs are normally controlled by a human operator and Human Machine Interfaces (HMIs) are important components of an ICS.

All these diverse components must communicate with other components of the ICS. To do so, they are often connected within "wired" communication architecture. Although wired connections render valuable reliable services to the infrastructure elements, nature or man-made disasters can damage the ICS wired communication infrastructure. It is just one of the reasons why wireless technologies—which we discuss in the Chap. 3—are gradually gaining popularity in ICS architectures, especially as ICS systems undergoing extensive upgrade efforts in the last few years. Still, replacement of wired communications with wireless is likely to continue at an accelerated pace. This is because incorporating wireless technologies into existing ICSs can bring many benefits including: (1) lowering installation costs and maintenance, (2) providing ad hoc on-demand deployment architecture that is robust and agile in responding to cyber and physical threats, and (3) providing redundancy, which is critically important in ICSs. In this chapter, as a case study, we discuss how an existing Smart Grid system could be integrated with the wireless technologies, focusing on the implementation of a real Smart Grid hardware/software testbed.

A modern ICS is a complex system that depends on many different components and technologies to monitor and control physical processes; along with many of the managerial, administrative, and regulatory responsibilities associated with this task. The computation and communication components within an ICS are often categorized into Operations Technology (OT) and IT based on the system functions they support. We discuss this categorization in the Chap. 4. Clearly, the key difference is that OT focuses on the monitoring and control of the physical process. This introduces substantial differences in how OT systems—as contrasted with IT systems—are operated and managed, along with the technologies used to support them.

After we explored the general nature of ICS and SCADA systems, in Chap. 5 we take a broad look at threats to these systems, i.e., the causes of cyber incidents. This chapter defines an ICS threat as "potential cause of an unwanted incident through the use of one of more ICSs, which may result in harm to individuals, a system, an organization, critical infrastructure and vital societal services, the environment or the society at large". Related to threat is vulnerability, which is defined as "weakness of an asset or control that can be exploited by one or more threats." The combination of ICS threats and vulnerabilities lead to the ICS risk and to a possibility of a successful attack.

Therefore in Chap. 6 we explore how threats enable specific attacks, and the classes and examples of attacks on such systems. The nature and efficacy of attacks are largely determined by a complex mix of security deficiencies in ICS systems that aggregate architectures and approaches from several epochs of technological history. For example, SCADA systems of the second generation were distributed, but used non-standard protocols. This enabled centralized supervisory servers and remote PLCs and RTUs. Security was often overlooked in this generation. The third generation of SCADA systems used common network protocols such as TCP/IP. This generation added the concept of Process Control Network (PCN), which allowed SCADA enclaves to connect to the Internet at large. The connection enabled operators to remotely manage the SCADA ecosystem but also introduced malware to the enclaves. To provide a more concrete sample context for discussion of such attacks, the chapter presents a notional system that captures key features of many SCADA systems. Finally, the chapter discusses Stuxnet—a well-studied and documented rootkit used on a SCADA system—in detail.

With many types of systems, elements, threats, attacks, vulnerabilities, threat actors and so on, it is natural to wonder whether some conceptual order could be imposed on the complex and seemingly chaotic space of ICS security. Taxonomies and ontologies are among means by which humans bring order, meaning and knowledge management to broad domains of things, concepts and principles. For this reason, in Chap. 7 we offer an overview of selected ICS security taxonomies and elements of emerging ontologies. Ontologies are already used in a variety of applications, from Search Engine Optimization, Knowledge Discovery (e.g., elicitation of patterns of interactions within genomic data), and traditional AI and common-sense reasoning. The use of ontologies to complement ICS security taxonomies is a logical extension.

To enhance the security of any system, and to defend it effectively, one must know the risks associated with failures of the system's security. Common definitions of risk typically talk about the likelihood of an undesirable event, and a measure of the impact of the event. Therefore, Chap. 8 focuses on the problems of cyber risk assessment and management, with emphasis on application to ICS analysis. There are important benefits in such quantifications of risks and risk mitigations. They open doors to comprehensive risk management decision-making, potentially highly rigorous and insightful. Quantification of risks can also contribute to rapid, automated or semi-automated implementation of remediation plans. The chapter includes a detailed example Petri net analysis of a hazardous liquid loading system process, its failure modes and costs associated with the failure modes.

Risk is the best known and perhaps the best studied example within a much broader class of cyber security metrics. However, risk is not the only possible cyber security metrics. Other metrics can exist and could be potentially very valuable to defenders of ICS systems. When used effectively, metrics can help to clarify one's understanding of the processes of a particular area of a system, and from there, provide information for external review and assist towards further improvement. In terms of cyber security metrics, ICSs tend to have unique features: in many cases, these systems are older technologies that were designed for functionality rather than security. Therefore, metrics for ICSs must be tailored to a diverse group of systems with have many features which were not necessarily built with connectivity and security in mind. For this reason, in Chap. 9, we first outline the general theory of performance metrics, and highlight examples from the cyber security domain and ICS in particular. We then focus on a particular example of a class of metrics—metrics of resilience. The chapter presents two approaches for the generation of metrics based on the concept of resilience using a matrix-based approach and a network-based approach. Finally, a discussion of the benefits and drawbacks of different methods is presented along with a process and tips intended to aid in devising effective metrics.

The next chapter—Chap. 10—explores the science, technology and practice of human perception, comprehension and projection of events and entities in cyber defense of ICS. The chapter delves into the scope of situational awareness (SA), and its roles in the success of the mission carried out by ICS or SCADA system support. Such control systems provide the cyber-physical-human couplings needed to collect information from various sensors and devices and provide a reporting and control interface for effective human-in-the-loop involvement in managing and securing the physical elements of production and critical infrastructure. The characteristics of ICS environments add additional considerations and challenges for human defenders. Cybersecurity operations typically require a human analyst to understand the network environment and the attackers. In defending ICS environment, however, an analyst must also understand the physical dimension of the ICS environment. This poses serious challenges to maintaining cybersecurity and SA as it spans the human, cyber, and physical dimensions and a myriad of possible interactions and exploits. Maintaining SA is critical to the cybersecurity of an ICS. This chapter addresses the specific challenges posed by the physical, cyber, and human dimensions that must be considered and understood in order for human analysts to best assess and understand the requirements to successfully defend against potential attacks.

Even if the threats, risk factors and other security metrics are well understood and effectively mitigated, a determined adversary will have non-negligible probability of successful penetration of the ICS. In the Chap. 11 we use the word "intrusion" to refer to a broad range of processes and effects associated with the presence and actions of malicious software in an ICS. Once an intrusion has occurred, the first and necessary step for defeat and remediation of the intrusion is to detect the existence of the intrusion. Much of the chapter's attention is on the difficult question of whether insights and approaches developed for IDS intended for ICT can be adapted for ICS. To answer this question, the chapter explores the modern intrusion detection techniques in ICT such as host-based techniques and network-based techniques, and the differences and relative advantages of signature-based and non-signature methods. We also introduce approaches based on an appreciable degree of knowledge about the process controlled by the ICS. These methods focus on monitoring the underlying process in the control system rather than monitoring network traffic. One of the methods presented in the chapter attempts to model process variable excursions beyond their appropriate ranges using machine-learning techniques. The second method requires plant personnel input to define critical process variable limits. Semantic modeling of plant control variables is used in both methods. The chapter concludes with a detailed case study of IDS in the context of a sample plant and its ICS.

In the following chapter—Chap. 12—we continue to explore the topic introduced in the previous chapter, but with a special focus on use of physical measurements for intrusion detection. We explain that monitoring the physical environment in the Field zone can get very valuable information, not only about the physical process (control), but also about the execution status of controllers and digital devices. Since field controllers ultimately determine the physical process, it is possible to obtain an indirect assessment of the integrity of the field devices my monitoring the process itself. This concept can be extended to the monitoring of the physical processes happening inside the controllers themselves, and in this way assess directly the execution status of the controllers. The chapter concludes with the case study of an implemented IDS system for a commonly used PLC. The IDS determines the baseline. Then, we introduce a malicious modification, similar in structure and operation to Stuxnet, into the PLC logic and the IDS uses the baseline to detect the intrusion.

Chapter 13 points out that the need for experimental approaches is particularly acute with respect to ICS cyber security. The ability to assess cyber posture, effectiveness, and impact for predictive analysis is predicated on the assumption that operators, users, and others have prior and complete understanding of the effects and impacts caused by cyber adversaries. Obviously, this is often not the case. When compared to the physical world, cyber is quite different, in that it does not follow physical scientific laws; rather, cyber is unbounded because it is a human-made science. As a result, understanding and quantifying effects are still an immature science. Many systems do not lend themselves to closed form mathematical solutions. Thus experimentation becomes a key method of performing analysis of these systems. In order to develop a foundation for identifying and bounding the issues, one approach to this problem is empirically through experimentation, much like physical sciences such as chemistry and physics.

In spite of decision support technologies, such as experimentation and simulation discussed in the previous chapter, it remains challenging for ICS stakeholders (leaders, managers, operators, etc.) to make informed decisions regarding formulating guidance, assigning responsibilities, balancing security and efficiency, allocating funding, determining return on investment, and measuring performance. Formulating and establishing an overarching plan that supports and guides such decisions is often called governance. This is the subject of Chap. 14.

Generally the term governance refers to processes of interaction and decision-making among the actors who collectively solve the problem such as ensuring and maintaining security of an ICSs. Governance includes actions and processes that engender and support stable practices and organizations. In the context of ICSs, such processes ensure that benefits of ICSs are delivered in a well controlled manner and are aligned with long-term goals and success of the enterprise. This chapter begins with an illustrative story, inspired by real-life experiences, which help the reader to appreciate some of the practical reasons for good governance of ICSs. Then the chapter describes the definitions, purposes and sources of governance. Because governance is particularly important for the purposes of ICS security assessments, the chapter continues by focusing on frameworks and methodologies that govern ICS assessments.

The next chapter—Chap. 15—reaches to a subject of potential active and military response to an attack on ICS performed by a nation state. A subject like this rarely if ever enters the purview of a typical ICS stakeholder. However, because ICS attacks are so likely to be perpetuated by a nation state, and because any response to an ICS attacks may touch on issues related to a hostile nation state, we feel that this book benefits from exploring this unusual topic. Evidence exists that nation-state actors have realized the utility of holding ICSs at risk; they have also demonstrated intent to gain and retain access to ICS networks, and a willingness to use such an access when deemed necessary. The chapter considers three case studies. The first case, made public in 2015, concerns the alleged episodes in which the Chinese government hacked into the computer networks of the U.S. Congress, Department of Defense, State Department, and major American corporations. The second is the Operation Cleaver in which Iranian state sponsored cyber actors have allegedly conducted several attacks against critical infrastructure. The third case explores the Havex malware, first reported in June 2014, which was presumably developed and distributed by a nation-state actor.

We chose to conclude this book with a look into the future of ICS cyber security. As best as we can see, much of this future unfolds in the context of the Internet of Things (IoT). In fact, we envision that all industrial and infrastructure environments, and CPSs in general, will take the form reminiscent of what today is referred to as the IoT. Therefore, the final chapter of the book is called *In Conclusion: The Future Internet of Things and Security of its Control Systems* (Chap. 16). IoT is envisioned as multitude of heterogeneous devices densely interconnected and communicating with the objective of accomplishing a diverse range of objectives, often collaboratively. One can argue that in the relatively near future, the IoT construct will subsume industrial plants, infrastructures, housing and other systems that today are controlled by ICS and SCADA systems. In the IoT environments, cybersecurity will derive largely from system agility, moving-target defenses, cybermaneuvering, and other autonomous or semi-autonomous behaviors. Cyber security of IoT may also benefit from new design methods for mixed-trusted systems; and from big data analytics—predictive and autonomous.

References

Cardenas, A.A. (2008). Secure control: Towards survivable cyber-physical systems. In *The 28th International Conference on Distributed Computing Systems Workshops* (pp. 495–500). IEEE.

Executive Order No. 13636. (2013). *Improving critical infrastructure cybersecurity*. Retrieved from http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf.

IEC TS 62443-1-1. (2009). *Security for industrial automation and control systems—Models and concepts*. IEC, International Electrotechnical Commission.

Stouffer, K., Lightman, S., Pillitteri, V., Abrams, M., & Hahn, A. (2015). *Guide to industrial control systems (ICS) security*. NIST Special Publication 800-82 Revision 2.

Knapp, E. D. (2012). Industrial control systems cybersecurity proof of concept. In *Department of Homeland Security Industrial Control Systems Joint Working Group Spring Conference, Savannah, GA*.

Krotofil, M. (2015). Rocking the pocket book: Hacking chemical plants. In *DefCon Conference, DEFCON*.

Langner, R. (2011). Stuxnet: Dissecting a cyberwarfare weapon. *IEEE Security & Privacy, 9*(3), 49–51.

Lüders, S. (2005). *Control systems under attack?* 10th ICALEPCS international conference on accelerator and large experimental physics control systems (pp. FR2.4–6O). Geneva: CERN. Retrieved November 8, 2015, from https://accelconf.web.cern.ch/accelconf/ica05/proceedings/pdf/O5_008.pdf.

NIST. (2014). *Framework for improving critical infrastructure cybersecurity*. NIST, National Institute of Standards and Technology.

Nizar, A.H. (2009). Identification and detection of electricity customer behaviour irregularities. In Nizar, A.H., & Dong, Z.Y. (Eds.), *Power systems conference and exposition. PSCE'09. IEEE/PES* (pp. 1–10). IEEE.

US Department of Energy. (2002). *21 steps to improve cyber security of SCADA networks*. Washington, DC: US Department of Energy. Retrieved from http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/21_Steps_-_SCADA.pdf.