How Industrial Control System Security Training is Falling Short

Jonathan Butts, Michael Glover

▶ **To cite this version:**

Jonathan Butts, Michael Glover. How Industrial Control System Security Training is Falling Short. 9th International Conference on Critical Infrastructure Protection (ICCIP), Mar 2015, Arlington, VA, United States. pp.135-149, 10.1007/978-3-319-26567-4_9 . hal-01431018

HAL Id: hal-01431018
https://inria.hal.science/hal-01431018

Submitted on 10 Jan 2017

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Distributed under a Creative Commons Attribution 4.0 International License

Chapter 9

HOW INDUSTRIAL CONTROL SYSTEM SECURITY TRAINING IS FALLING SHORT

Jonathan Butts and Michael Glover

Abstract Industrial control systems monitor and manage critical infrastructure assets. Every sector relies extensively on the proper operation of control systems and a major disruption could have devastating consequences to the economy and society. Protecting industrial control systems requires large numbers of well-trained security personnel to detect and respond to increasingly sophisticated cyber attacks. This chapter evaluates current government and industry training courses in the area of industrial control systems security. The results indicate that training is typically geared towards the basic or intermediate knowledge levels and that adequate advanced training programs are not readily available. A primary deficiency is the lack of robust training facilities that incorporate real critical infrastructure assets. Additionally, the curricula do not sufficiently incorporate the physical components and processes associated with industrial control systems. Indeed, there is a great need for training facilities that incorporate real-world industrial control systems and processes to provide trainees with a strong understanding of the effects that cyber-initiated actions have on physical processes. While major investments are required to create advanced curricula and training facilities, they will contribute significantly to the important task of protecting the critical infrastructure.

Keywords: Industrial control systems, training, facilities, curricula

1. Introduction

Industrial control systems (ICSs) monitor and manage critical infrastructures such as the electric power grid, water treatment systems, oil and gas pipelines, and chemical and nuclear plants. In recent years, industrial control systems have increasingly become interconnected with enterprise networks and the Internet to take advantage of cost savings and operational benefits. This

trend, however, has introduced myriad attack entry points associated with the networking environment. As a result, formerly isolated critical infrastructure assets are now susceptible to a wide range of threats that previously did not exist. Exacerbating the concern is that approximately 85% of the U.S. critical infrastructure is privately owned and operated [7].

Unfortunately, the majority of infrastructure owners and operators – especially private entities and municipalities – do not understand the risks and have minimal capabilities to respond to sophisticated cyber attacks that target industrial control systems. Training programs are primarily focused on information and communications security rather than industrial control system security.

This chapter evaluates government and industry training programs that specifically focus on industrial control system security professionals. The results indicate that deficiencies exist with respect to training facilities and curricula. Additionally, the training programs do not incorporate coordinated efforts for responding to targeted attacks against critical infrastructure sectors. To overcome the deficiencies, regional facilities are recommended that would support industrial control system security training that utilizes real-world systems. Due to the significant costs and coordination that will be involved, active federal government sponsorship and participation will be required. However, these investments are needed to ensure that adequate numbers of trained personnel are available to prevent and respond to cyber attacks that target industrial control systems and, by extension, the critical infrastructure.

2. Background

Coordinated cyber attacks target two primary categories of computing systems: (i) traditional information and communications technology (ICT) systems; and (ii) cyber-physical systems [9]. Note that, although the fundamental principles for exploiting the two categories of computing systems may overlap, the effects of cyber-initiated actions on these two types of systems are quite different. Information and communications technology includes systems and applications associated with computer and network hardware, software and communications media [6]. The technology encompasses computers, enterprise software, middleware and data storage that enable users to access, manipulate, store and transmit information. The exploitation of information and communications systems can result in the loss of sensitive or proprietary information, degraded communications, loss or unavailability of data processing and computing systems, and data manipulation. Cyber-physical systems comprise embedded devices and are system-of-systems that are typically associated with the critical infrastructure. Cyber-physical systems, such as industrial control systems, are designed for the "seamless integration of computational algorithms and physical components" [2]. Attacks on these systems can achieve direct kinetic effects that could result in equipment damage and the loss of human life.

Due to the extensive private ownership of the critical infrastructure, the government must largely rely on civilian personnel to protect these national assets. It is imperative that these personnel are adequately trained to protect against, respond to and recover from cyber-initiated attacks on critical infrastructure systems.

Due to the increased threats to the critical infrastructure, myriad courses have been developed to help train control system security professionals in government and industry. In this discussion, only training courses that are publicly available to security professionals are considered.

Government training on industrial control system security is primarily offered by the Department of Homeland Security (DHS) and the Department of Energy (DoE) National Laboratories [4, 8]. The courses incorporate lectures and hands-on training focused on how attacks are launched, why they work and how to develop mitigation strategies. The topics include reviews of industrial control system security, comparative analysis of information and communications system and industrial control system architectures, security vulnerabilities and mitigation strategies. The DHS ICS-CERT advanced training course uses a representative industrial control system to demonstrate how exploits can affect process systems and the utility of mitigation solutions. The training culminates in a red team/blue team exercise that divides students into teams of attackers and teams of defenders. Students are expected to have a strong understanding of industrial control networks and information and communications networks in order to register for the course. The hands-on course is offered only at specific locations in the United States and students must to travel to one of the sites to take the course.

Industry training is primarily offered in the form of one-week courses conducted by vendors. Although a number of vendors offer industrial control system security training, the curricular outlines and training environments are quite similar. The topics covered include industrial control system fundamentals, assessing and managing risk, auditing and assessing systems, defense strategies and implementing security controls. The majority of training courses offer hands-on laboratory assignments that incorporate components such as programmable logic controllers (PLCs) that may be networked in a simulated operational environment. Instructors typically travel to various locations to conduct the training courses, although on-site training tailored to individual organizations is also available. Some vendors offer training at facilities that incorporate simulation testbeds and table-top experimental set-ups that are representative of real industrial control systems. Trainees have a wide range of backgrounds and typically no prerequisites are required to attend the courses.

3. Gap Analysis

A gap analysis was performed to examine industrial control system security training requirements and existing capabilities. The following shortfalls were identified:

- **Training Facilities:** The primary shortfall is the lack of appropriate training facilities. A training facility must incorporate real-world systems that adequately prepare students to deal with the situations encountered in industrial environments. Current training facilities either engage simulations or systems that are scaled-down models of physical processes. A real-world, high-fidelity training facility is often overlooked or is considered to be impractical due to the extensive costs associated with incorporating full-scale systems and physical processes. As a result, the courses only provide an abstract understanding of the systems and the associated attacks and defensive strategies. It is imperative that training programs offer hands-on experience and immersion in actual industrial control environments. Without the incorporation of actual physical processes and full-scale systems in training programs, it is impossible for trainees to acquire the skills needed to operate industrial processes in the face of attacks and failures that emanate from the cyber domain.

- **Training Curricula:** The primary gap in training curricula is the lack of emphasis on physical processes. Current training programs focus primarily on defending and exploiting traditional information and communications systems; they do not adequately incorporate the physical components and processes that are encountered in industrial environments. As a result, the courses do not provide a strong understanding of the implications of cyber-physical correlations and the effects that cyber actions have on physical controls and instrumentation. Although the curricula may offer foundational training, they are not tailored to provide the advanced skills required to detect and mitigate attacks on critical infrastructure assets.

3.1 Training Facility Evaluation

A robust training facility is the key to developing industrial control system security specialists. The training facility must incorporate real-world process systems and control systems and provide hands-on experience. Testbeds and simulation environments may be used to supplement real-world learning experiences, but it is important to be cognizant of the fact that they do not adequately reflect real-world system implementations.

One of the primary challenges when creating a training facility is the integration of a full-scale industrial control system. Real-world industrial control systems comprise equipment from a number of vendors and use diverse protocols, configurations and instrumentation. As a result, the costs associated with designing and implementing a realistic training facility are significant. However, training on real-world industrial control systems exposes personnel to the configuration and deployment intricacies encountered in industrial environments. Additionally, the use of real-world systems emphasizes the importance of physical-safety-override systems and how they affect functionality.

Table 1. Industrial control system (ICS) training environments.

	Government	Industry
Individual ICS Subcomponents	A	A
Interconnected ICS Subcomponents	P	P
Real-World Cyber-Physical Interactions	P	P
Full-Scale Functional ICSs	–	–
Incorporation of Safety Systems	–	–
Ability to Assess Multiple Access Points	–	P
Ability to Manipulate Physical Processes	P	P
Ability to Measure Effects	P	P
Remote Control Center	P	–
Modular Training Environment	–	–
Multiple Vendor Exposure	–	P
Multiple Communications Media	–	P
Interactive Training Capability	P	P

Requirements. A training facility that incorporates real-world industrial control systems is needed to ensure that trainees acquire an in-depth understanding of industrial control systems and the effects that cyber-initiated actions have on physical processes. Simulated environments and small-scale testbeds simply do not provide the required functionality, processes or physical components.

Analysis of Existing Capabilities. Several leading government and industry training facilities were evaluated to assess their ability to support industrial control system training objectives. Table 1 summarizes the findings. Note that "A" indicates that training facilities adequately cover the requirement while "P" indicates that the requirement is partially covered.

Current training facilities lack real-world systems and the ability to manipulate physical processes and measure effects. To meet industrial control system training requirements, personnel must be exposed to hands-on training that incorporates real physical systems. Current training facilities primarily use individual components, simulated environments or small-scale testbeds – the vast majority of facilities use only individual subcomponents. Some of the more advanced training facilities incorporate simulations for traffic generation and provide notional targets for practicing exploitation and defense. A few training facilities offer small-scale testbeds that model real-world systems and provide opportunities to manipulate physical devices and observe minor effects. It is important to note, however, that the testbeds provide only a fraction of real-world functionality and do not adequately replicate the processes, interactions and sophistication associated with fully operational systems. Even at the most basic level, trainees must be exposed to functioning systems to observe the physical processes and control systems in operation and to gain insight into

their complex behavior. Unfortunately, it is often the case that trainees never get to see, let alone experiment with, operational industrial control systems.

The majority of training courses use control system subcomponents and virtualized applications for training. For example, trainees are often assigned programmable logic controllers for the duration of a course, but the controllers typically have limited or no interconnections to other control system components. Additionally, the training may not incorporate a remote control center, which is a core component of industrial control systems and one that is frequently targeted by attackers. In many instances, the training facility fails to incorporate key components such as human-machine interfaces, historians and input/output servers. A training facility should incorporate a variety of common access points to expose trainees to methods for gaining unauthorized access to industrial control systems. For example, a primary training requirement should be the ability to identify industrial control system subcomponents from within a corporate network, understand how to pivot and then gain access to the control network.

Communications infrastructures provide different attack vectors and can also alter the operating characteristics of industrial control systems. A training facility should incorporate the range of communications infrastructures that are likely to be encountered in operational environments. The training facility should provide modularity to create the different configurations that meet training objectives, advance student skills and replicate the myriad environments encountered in real-world infrastructures. Most training courses use simulations or testbeds that focus on single, isolated instances of systems. It is important that training courses provide professional with opportunities to work on multiple types of systems used in the various infrastructure sectors.

Well-trained industrial control system professionals should be knowledgeable about how cyber actions can manipulate physical processes and how altering physical processes can affect the cyber components. For example, several cyber options may be available to achieve a desired effect such as shutting down power to a targeted area – these include the available access, types of field devices, operating systems and applications, available exploits and system configurations. It is also critical that a specialist understands and can identify the various risks to individual system components as well as the system as a whole.

3.2 Training Curricula Evaluation

Industrial control system training curricula must prepare professionals for the range of threats that are likely to be encountered when operating critical infrastructure assets. The research results indicate that that training programs are generally inadequate – they primarily focus on exploiting and defending conventional information and communications systems and do not sufficiently incorporate physical components and process systems. A well-designed training program must emphasize the physical aspects and effects associated with industrial control systems.

A professional with strong expertise in process systems and cyber capabilities has the ability to identify the range of threats, comprehend their implications, articulate the strengths and weaknesses of mitigation options and perform the appropriate actions. Indeed, understanding the many ways in which a cyber attack can alter a physical process provides the insight needed to develop and apply strategies to protect against system manipulation. If a physical process has been altered, an experienced operator should be able to discern if the physical effect was cyber-initiated, identify attack vectors, determine the risks to other components and systems, modify configurations and parameters to minimize operational impact and eliminate the threat.

Requirements. Industrial control system security training must provide comprehensive knowledge of the cyber components and physical processes. It is woefully inadequate to understand just the cyber components or physical processes when defending against targeted attacks. In industrial environments, cyber professionals and control engineers have historically been segregated, with each group focusing on its specific area of expertise [3]. The separation of duties and responsibilities has resulted in a lack of understanding of the holistic functionality of industrial control systems. The incorporation of sophisticated automation technologies in industrial environments means that definitive lines cannot be drawn between the engineering aspects of the physical processes and the cyber aspects. This is similar to the case of an automobile technician who, due to advancements in technology, must have knowledge of and the ability to work on the mechanical and electrical systems of modern automobiles.

Industrial control system security specialists must have the ability to analyze a system, understand its functionality, comprehend the risks, evaluate potential secondary effects and articulate mitigation strategies. The core knowledge areas for training curricula that would meet these requirements are: (i) industrial control system principles; (ii) cyber manipulation; and (iii) response coordination. The knowledge areas corresponding to the three core areas are:

- **Industrial Control System Principles:**
  - System functionality
  - Control theory
  - System architecture and operating requirements
  - Instrumentation devices
  - Field device components
  - Control and data acquisition
  - System applications
  - Communications and interconnections
  - Real-world configuration and deployment

- **Cyber Manipulation:**
  - Industrial control systems versus information and communications systems
  - Access vectors
  - Asset enumeration and identification
  - Field device, application and operating system analysis
  - Communications and protocol analysis
  - Vulnerability analysis
  - Availability, integrity and confidentiality
  - Exploitation
  - Pivoting
  - Implanting malware
  - Manipulating physical processes
  - Network protection
  - Forensics
  - Hardening strategies
- **Response Coordination:**
  - Prioritizing system components
  - Identifying attacks
  - Determining system impact
  - Minimizing impact
  - Eradicating malware
  - Recovering from attacks
  - Determining the root cause
  - Implementing safeguards to prevent recurrence
  - Analyzing attacks to obtain intelligence and insights
  - Evaluating defense strategies

The knowledge areas were derived from the skill-set required to defend against targeted attacks on industrial control systems. A specialist should understand: system operating principles; components and functionality; underlying physical processes; cyber-physical correlations; means for gaining access to cyber-physical systems; implications of cyber actions on physical processes; how cyber capabilities are leveraged to achieve physical effects; how to evaluate second-order and cascading effects; limitations of cyber capabilities; and how cyber-kinetic actions are incorporated into requirements, planning and operations.

Table 2. Industrial control system (ICS) training curricula.

	Government	Industry
ICS Fundamentals	B	B
Control Theory	–	B
ICS System Architecture	B	B
Physical Controls	–	–
Instrumentation	–	B
Field Device Operations and Programming	B	I
Control and Data Acquisition	B	B
ICS System Applications	B	I
Communications Media and Protocols	B	I
Implications of Safety Systems	–	B
System Effect Analysis	B	B
ICS vs. ICT Exploitation	A	A
Asset Enumeration and Identification	B	I
Access Vectors	B	B
Field Device and Application Analysis	B	I
Operating System Analysis	I	A
Vulnerability Analysis	B	I
Exploitation	I	I
Pivoting	B	B
Implanting Malware	–	B
Physical Process Manipulation	B	B
Forensics	B	B
Hardening Strategies	I	I
Asset Prioritization	–	–
Time Factors	–	–
Second-Order Effects	–	–
Malware Eradication	–	B
Minimizing Operational Impact	–	–
Response and Recovery Actions	B	B

Analysis of Existing Capabilities. Several government and industry training programs for industrial control system security were evaluated. The training curricula were mapped to the core knowledge areas to identify shortfalls. Table 2 summarizes the findings. Note that "B" indicates that training is available that covers the requirements at a basic level with no practical applications; "I" indicates that training is available that covers the requirements at an intermediate level with practical applications; and "A" indicates that training is available that covers the requirements at an advanced level with in-depth practical applications.

The findings revealed little variance in the training courses with regard to industrial control system fundamentals and cyber manipulation. The primary gaps for all the training courses include the lack of emphasis and material relating to physical systems, instrumentation, safety systems and system effect

analysis. From the knowledge and skills perspective, the course material ranged primarily from the beginner level to the intermediate level.

A common theme identified during the curriculum analysis was the traditional information and communications system penetration testing (assessment) mentality. Traditional information and communications system assessments involve a network focus, freedom to maneuver to discover vulnerabilities, a known environment (e.g., Windows operating system) and common vulnerabilities discovered via network assessment tools. Although industrial control systems comprise traditional information and communications systems, understanding how targeted physical effects are achieved requires an evaluation of the overall system-of-systems architecture beyond just the cyber aspects. Current training programs examine individual subcomponents in isolation and do not adequately consider the holistic system. It is imperative that programs cover the interactions between subcomponents and how manipulating parameters in one subsystem or device can cascade throughout a system.

Current training programs rarely go beyond the basic programming and functionality of industrial control system subcomponents. Also, communications protocols are analyzed at a functional level and only a few protocols are incorporated in the training regimens. As a result, there is a major gap related to the implications of the cyber-physical correlations and the effects that cyber actions have on physical controls and instrumentation. Indeed, most training programs are geared towards information and communications technology professionals and primarily expose them to control system functionality and security threats. Although the curricula do help develop awareness and provide basic knowledge, they are not tailored to impart advanced knowledge and skills. As a result, the training programs mainly prepare individuals to protect against attacks directed at information and communications systems instead of preparing them to address sophisticated, targeted attacks on control systems and the infrastructures they operate.

4. Recommendations

The recommendations are focused on delivering training programs that meet the requirements associated with securing critical infrastructure assets across the various sectors. As an initial step, investments must be made to develop realistic training facilities. Curricula should also be developed, ideally through government sponsorship and public-private cooperation, that would provide the best possible training.

4.1 Training Facilities

The primary obstacle to providing adequate training is a sufficient number of facilities that incorporate real-world control systems and processes. These facilities would support the delivery of intense hands-on courses that would enable trainees to observe and learn from the effects of real attacks on industrial control systems. To truly understand the security implications and

response strategies, real-world environments are required that comprise multiple interconnected systems (e.g., oil and gas, electric power, water/wastewater and building automation systems).

To overcome the deficiencies, it is recommended to construct several regional facilities that would support industrial control system security training on real-world systems. The primary challenges are the significant costs and coordination that will be required to deploy and operate these facilities. To address these challenges, active federal government sponsorship and participation is required (it would be exceedingly difficult for private entities to independently fund and operate large-scale facilities). Indeed, the Departments of Homeland Security, Energy and Defense, the Government Accounting Office and other government organizations have a vested interest in industrial control system security. The federal government can leverage critical infrastructure assets at legacy sites (e.g., closed military bases) to develop real-world training environments. The various regional training facilities could focus on different combinations of critical infrastructures.

4.2 Training Curricula

Intense training courses that incorporate actual physical systems are required. The proposed training curriculum should cover three core areas: (i) industrial control system principles; (ii) cyber manipulation; (iii) and response coordination. The industrial control system principles and cyber manipulation areas are divided into specific training blocks aligned to the required knowledge and skill sets. The response coordination core area focuses on the practical application of knowledge gained from the industrial control system principles and cyber manipulation core areas. Table 3 lists the recommended course topics.

Industrial Control System Principles. The industrial control system principles core area focuses on physical system attributes and cyber-physical relationships. System functionality includes operating principles, the common vernacular and implementation details in the various sectors. Control theory provides the fundamental knowledge of processes, control systems, systems dynamics and systems engineering required to understand system function and design specifications. System architecture and operating requirements detail the types of configurations and parameters that support system functionality. Note that system functionality is dependent on the underlying physical process. For example, a liquid pipeline has strict timing requirements because liquid is incompressible and an increase in pressure due to a blockage could result in a pipeline rupture, whereas a gas pipeline has less restrictive timing requirements because gas is compressible [1]. Deep knowledge about such system properties is critical to understanding and mitigating the effects of attacks.

Instrumentation devices measure physical system properties such as temperature, pressure, flow and level. It is important to understand how the current and voltage input/output signals to/from field devices impact sensors and actuators that instantiate the physical changes in the process system. Under-

Table 3. Industrial control system (ICS) course topics.

CORE I: Industrial Control System Principles
Block I: Fundamentals
Block II: Physical Systems and Instrumentation
Block III: Field Devices
Block IV: Industrial Control System Software
Block V: Communications
Block VI: Advanced Control
CORE II: Cyber Manipulation
Block I: Familiarization
Block II: System Profile
Block III: Vulnerability Analysis and Exploitation
Block IV: Defending Against Attacks
CORE III: Response Coordination
Block I: Coordination of Internal and External Responses
Block II: Prioritization of System Components
Block III: Determination of System Impact
Block IV: Minimization of System Impact
Block V: Determination of the Root Cause
Block VI: Eradication of the Cause
Block VII: Implementation of Recovery Strategies

standing the programming languages and field device system architecture (i.e., hardware, firmware and software) provides the ability to manipulate system control via device exploitation. Control and data acquisition covers system interaction and how data is processed and used throughout the system. Applications includes programs for managing system functionality, providing process visualization and enabling operator interfaces. Knowledge of communications protocols, network design and topology are critical to determining access capabilities and how network traffic is routed.

Cyber Manipulation. The cyber manipulation core area emphasizes the ability to defend against exploitations of cyber vulnerabilities that affect a physical process. It is important to understand the differences between traditional information and communications systems and industrial control systems. Fundamentally, the methods for identifying vulnerabilities in hardware, software or system configurations do not change; however, the exploitation of a vulnerability and the resulting impact are highly dependent on the targeted system. For example, scanning a traditional IP network can identify and provide details of the workstations in the network. On the other hand, performing a similar scan on an industrial control network can cause field devices to malfunction and potentially render them inoperable [5]. It is important to know how to obtain system configuration data and parameters, as well as to understand the capabilities and limitations of available tools.

Understanding access vectors provides insights into leveraging communications systems and other access points to gain entry to industrial control systems. Asset enumeration and identification helps discern the components that comprise a system, including their technical details and network interconnections. This information is used to analyze field devices, applications, operating systems, communications and protocols and determine system configuration and software/firmware information. A vulnerability analysis reveals weaknesses in system configuration, design and implementation for exploitation and implanting malware. Confidentiality, integrity and availability considerations help determine how attacks can manipulate physical processes. Pivoting involves leveraging access gained to one system to compromise other systems. In the case of industrial control systems, pivoting enables attackers to access appropriate subcomponents to achieve their desired effects. Defensive capabilities ensure appropriate configurations and that safeguards are implemented to prevent compromise or minimize damage to the physical process should an attack occur. Forensic capabilities help determine how an attack occurred, the extent of damage and preventive measures to prevent future compromises, as well as obtain intelligence about the attack.

Response Coordination. Knowledge of response coordination is best obtained through mission-oriented training that immerses trainees in environments that mirror real-world operations and scenarios. The response coordination core area involves the application of industrial control system and cyber manipulation knowledge to tailored missions that emphasize the consideration of combined effects, determination of second-order effects and communications with internal and external agencies.

Defending systems against attacks and recovering from attacks require the prioritization of assets to ensure that the physical processes continue to operate as intended. Safeguards should be in place prior to attacks and routine assessments should be performed to identify weaknesses. After an attack is identified, the system impact should be analyzed to prevent or minimize further damage. Recovering from an attack requires the ability to determine the root cause, eradicate malware if it is present and prevent the recurrence of the attack. Digital forensic capabilities are required to understand the details of an attack and its impact as well as gain intelligence about the attack and attacker.

The recommended training curriculum is tailored specifically to meet industrial control system requirements. Each training module should combine classroom lectures with significant hands-on laboratory projects. The training should begin with modules that cover industrial control system principles and provide exposure to actual systems and subcomponents. The next set of modules should cover control engineering principles and control theory, system design, instrumentation and the programming and configuration of field devices, applications and interfaces. Following this, the training should cover the intricacies associated with cyber attacks on industrial control systems and how targeted effects are achieved through cyber-initiated actions that manipulate

physical processes. The training should also cover the prioritization of assets, defense strategies and recovery. The training should culminate in mission-oriented activities that apply the knowledge gained in real-world scenarios tailored to industrial control operations.

5. Conclusions

Advanced training is required to ensure that cyber security and industrial control professionals can respond appropriately to sophisticated cyber attacks on industrial control systems and the critical infrastructure assets they monitor and operate. The evaluation of existing government and industry training courses has revealed shortfalls with regard to training facilities and training curricula. Current industrial control system security training relies on individual components, simulated environments or small-scale testbeds. Although these may be effective for beginner and intermediate levels of training, they are inadequate for advanced training, which must provide strong hands-on experience with real industrial control systems and physical processes. Unfortunately, current training facilities have few, if any, real-world systems and do not provide the ability to manipulate physical processes and measure attack impact.

To overcome the deficiencies, regional facilities are recommended that would support industrial control system security training that utilizes real-world systems. The training curricula should cover industrial control system principles, cyber manipulation and response coordination in learning environments that blend classroom lectures with hands-on projects involving real control systems and physical processes. Due to the significant costs and coordination that will be involved, active federal government sponsorship and participation are recommended. These investments are needed to ensure that adequate numbers of trained personnel are available to prevent and respond to cyber attacks that target industrial control systems and, by extension, the critical infrastructure.

Note that the views expressed in this chapter are those of the authors and do not reflect the official policy or position of the U.S. Department of Defense or U.S. Government.

Acknowledgement

This research was partially supported by the Office of the Under Secretary of Defense for Personnel and Readiness.

References

[1] J. Couper, W. Penney and J. Fair, *Chemical Process Equipment: Selection and Design*, Butterworth-Heinemann, Waltham, Massachusetts, 2012.

[2] National Science Foundation, Cyber-Physical Systems, Program Solicitation, NSF 14-542, Arlington, Virginia (`www.nsf.gov/pubs/2014/nsf14542/nsf14542.htm`), 2014.

[3] L. Neitzel and B. Huba, Top ten differences between ICS and IT cybersecurity, *InTech*, International Society of Automation, Research Triangle Park, North Carolina, May/June 2014.

[4] Sandia National Laboratories, SCADA Training Courses, Albuquerque, New Mexico (`energy.sandia.gov/energy/ssrei/gridmod/cyber-security-for-electric-infrastructure/scada-systems/education-and-training/training-courses`), 2014.

[5] K. Stouffer, J. Falco and K. Scarfone, Guide to Industrial Control Systems (ICS) Security, Special Publication 800-82, National Institute of Standards and Technology, Gaithersburg, Maryland, 2011.

[6] U.S. Department of Defense, Protection of Mission Critical Functions to Achieve Trusted Systems and Networks, Instruction No. 5200.44, Washington, DC, 2012.

[7] U.S. Department of Homeland Security, Critical Infrastructure Sector Partnerships, Washington, DC (`www.dhs.gov/critical-infrastructure-sector-partnerships`), 2015.

[8] U.S. Department of Homeland Security, Training Available Through ICS-CERT, Washington, DC (`ics-cert.us-cert.gov/Training-Available-Through-ICS-CERT`), 2015.

[9] B. Zhu, A. Joseph and S. Sastry, A taxonomy of cyber attacks on SCADA systems, *Proceedings of the International Conference on the Internet of Things and the Fourth International Conference on Cyber, Physical and Social Computing*, pp. 380–388, 2011.