Oct 20th, 11:55 AM - 12:20 PM

Laboratory Exercises to Accompany Industrial Control and Embedded Systems Security Curriculum Modules

Gretchen Richards
Jacksonville State University

Abstract
The daily intrusion attempts and attacks on industrial control systems (ICS) and embedded systems (ES) underscore the criticality of the protection of our Critical Infrastructures (CIs). As recent as mid-July 2018, numerous reports on the infiltration of US utility control rooms by Russian hackers have been published. These successful infiltration and possible manipulation of the utility companies could easily translate to a devastating attack on our nation's power grid and, consequently, our economy and well-being. Indeed, the need to secure the control and embedded systems which operate our CIs has never been so pronounced. In our attempt to address this critical need, we designed, developed and implemented ICS and ES security curriculum modules with pertinent hands-on laboratory exercises that can be freely adopted across the national setting. This paper describes in detail the modules and the accompanying exercises and proposes future enhancements and extensions to these pedagogical instruments. It highlights the interaction between control and embedded systems security with Presidential Policy Directive 8- the National Preparedness Plan (NPP), cyber risk management, incident handling. To establish the premise the laboratory exercises were developed. This paper outlines the description and content of the modules in the areas of (1) Industrial Control Systems (ICS) Security, (2) embedded systems (ES), and (3) guidelines, standards, and policy.

The ICS security modules cover the predominant ICS protocols, ladder logic programming, Human Machine Interface (HMI), defensive techniques, ICS reconnaissance, vulnerability assessment, Intrusion detection, and penetration testing. The ES security modules include topics such as secure firmware programming and authentication mechanisms. In the guidelines, standards, and policy section, the topics covered by the modules include the NPP as it relates to CI protection, risk management, system protection and policy design, and managing operations and controls. An overview of the various hands-on exercises that accompany the course modules is also presented. Further, to evaluate the effectiveness of the pedagogical materials, an initial evaluation was conducted and the survey data were collected, analyzed, and presented. The paper concludes with future enhancements and directives on opportunities for module extensions and course adoption.

Location
KC 400

Disciplines
Information Security | Management Information Systems | Technology and Innovation

Laboratory Exercises to Accompany Industrial Control and Embedded Systems Security Curriculum Modules

ABSTRACT

The daily intrusion attempts and attacks on industrial control systems (ICS) and embedded systems (ES) underscore the criticality of the protection of our Critical Infrastructures (CIs). As recent as mid-July 2018, numerous reports on the infiltration of US utility control rooms by Russian hackers have been published. These successful infiltration and possible manipulation of the utility companies could easily translate to a devastating attack on our nation's power grid and, consequently, our economy and well-being. Indeed, the need to secure the control and embedded systems which operate our CIs has never been so pronounced. In our attempt to address this critical need, we designed, developed and implemented ICS and ES security curriculum modules with pertinent hands-on laboratory exercises that can be freely adopted across the national setting. This paper describes in detail the modules and the accompanying exercises and proposes future enhancements and extensions to these pedagogical instruments. It highlights the interaction between control and embedded systems security with Presidential Policy Directive 8- the National Preparedness Plan (NPP), cyber risk management, incident handling. To establish the premise the laboratory exercises were developed. This paper outlines the description and content of the modules in the areas of (1) Industrial Control Systems (ICS) Security, (2) embedded systems (ES), and (3) guidelines, standards, and policy.

The ICS security modules cover the predominant ICS protocols, ladder logic programming, Human Machine Interface (HMI), defensive techniques, ICS reconnaissance, vulnerability assessment, Intrusion detection, and penetration testing. The ES security modules include topics such as secure firmware programming and authentication mechanisms. In the guidelines, standards, and policy section, the topics covered by the modules include the NPP as it relates to CI protection, risk management, system protection and policy design, and managing operations and controls. An overview of the various hands-on exercises that accompany the course modules is also presented. Further, to evaluate the effectiveness of the pedagogical materials, an initial evaluation was conducted and the survey data were collected, analyzed, and presented. The paper concludes with future enhancements and directives on opportunities for module extensions and course adoption.

Keywords: Industrial Control Systems, Embedded Systems, Security, Laboratory Exercises, Curriculum Modules, Critical Infrastructures, Cyber Attack, Policy, Guideline, Regulatory Compliance

INTRODUCTION

In June 2017, the National Institute of Standards and Technology (NIST) published the first revision to the NIST SP 800-12 document, which contains guidelines that addresses the assessment and analysis of security control effectiveness and security posture of an organization

(Nieles, Dempsey, Kelley, & Pillitteri, 2017) (NIST SP800-12r1). In early 2015, the U.S. Department of Energy's Office of Electricity Delivery and Energy Reliability published a document titled "Energy Sector Cybersecurity Framework Implementation Guidance" (DOE, 2015) in response to NIST's Framework for Improving Critical Infrastructure Cybersecurity (NIST, 2014). Almost invariably, the North American Electric Reliability Corporation (NERC) continues to update and enforce a suite of Critical Infrastructure Protection (CIP) (NERC, 2015) standards related to the reliability of cybersecurity.

These guidelines and standards underscore the importance of protecting our critical infrastructures which are mostly operating through automated controlled systems. In an almost daily basis, this national need for cybersecurity-related CIP becomes more pronounced in light of intrusions and attempted attacks on Internet-facing control systems. As documented in (ICS-CERT, 2015), the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) responded to 245 incidents reported by asset owners and industry partners in 2014.

The rest of the paper is organized into five parts. First, we present background materials and the motivation behind this work. Second, we provide details on the design and implementation of Embedded Systems (ES) and Industrial Control Systems (ICS) security curriculum resources. Third, we describe the laboratory setup and the associated hardware wherein the exercises are conducted. Fourth, we describe in detail the laboratory activities pertinent to each module and present the results of the initial evaluation the pedagogical materials. Finally, we provide concluding remarks and present directions to possible extensions to this work.

BACKGROUND

Recognizing the need to protect our critical infrastructures from intended or unintended harm, we embark on an Embedded System (ES) and Industrial Control System (ICS) Security curricula enhancement project with the following objectives:

- to develop and enhance curriculum modules focused on embedded and industrial control systems security,
- to develop hands-on exercises to support the ES and ICS security learning modules,
- to present lessons learned at various information security conferences and to offer mini-training workshops to widely disseminate the learning module to the Center for Academic Excellence (CAE) community, and
- to evaluate teaching and learning effectiveness of the ES and ICS security curricula.

A professional development workshop on ICS security was conducted in June 2017 for college instructors. Overall, the pre- and post-workshop surveys indicate that the topics for the workshop were well-chosen and well delivered, and the inexpensive control systems hardware was rated as excellent. The results highlight that ICS security is a topic that is not well-covered in information assurance/cyber security curricula and the workshop, as intended, highlighted the importance of that and other aspects of cyber security and provided instructors with tools and knowledge to integrate ICS security into their courses. Interesting remarks, coming from two of the participants, indicate that our workshop is far superior to the recently attended PLC training workshop that was

offered by one of the biggest industrial control manufacturers in the country. The on-going project will build on the success of the recently concluded ICS workshop to effectively fill a void in cyber security training for the CAE community and to the Department of Defense (DoD) training personnel across the nation. It will have significant contributions to the Cybersecurity National Action Plan (CNAP) on addressing the expansion of the national cybersecurity workforce. As previously mentioned, ES and ICS security education, which is critical to our national interest, has lagged behind other cyber-related curricula due to the limited access to ICS/SCADA equipment and testbed facility. Obviously, ICS security hands-on training programs cannot be performed on operational ICS without disrupting normal operating processes and thus, the need for hands-on activities that are adequately supplemented by an inexpensive embedded and control system hardware similar to that used in this project is paramount.

Prior and Similar Works

There have been similar efforts to address the need for enhancing control systems security. Prior and notable related works that this project builds upon are found in Francia & Snellen, (2014), Thornton, Francia, & Brookshire (2012), and Francia & Francia (2014). A national Supervisory Control and Data Acquisition (SCADA) test bed program has been established by the Department of Energy (INL, 2014). A primary goal of the program is to provide control system security training through workshops. Although these workshops provided the necessary training for various individuals and groups, the training materials are not directly adaptable to rapid training of DoD personnel. The Cyber Security Education Consortium (CSEC) has created centers of excellence in automation and control systems to provide training on SCADA and control systems security (CSEC, 2014). The courses that were created for this security curriculum are excellent training tools to upgrade the security skills of operators. However, widespread adoption is restricted by the high cost and the lack of hardware resources to support the courses in a portable and affordable setting. The SANS Institute offers a course on Industrial Control Systems and SCADA Security (SANS, 2014) which targets those personnel who are directly involved with the operation of industrial controls. The exorbitant registration cost for the course makes it impractical for training workshop adoption. Our proposed capacity building project offers freely available course modules using affordable resources that can deliver hands-on and realistic control systems security training and education.

SECURITY CURRICULUM MODULES

The Industrial Control Systems (ICS) Security Curriculum Modules

Given the constraint that ICS curriculum modules must be designed to be self-contained as much as possible, we strived to cover the four basic areas of control systems application and security: Control system networks and protocols, Programmable Logic Controller (PLC) programming, Human Machine Interface (HMI) and System Historian development and security, control system vulnerability assessment and penetration testing, and defensive techniques and incident response for control systems. These modules are detailed in Table 1.

Table 1. The Control System Security Curriculum Modules

Module Name: Control System Networks and Protocols; Python Programming Learning Objectives: To understand control system networking concepts and communication protocols. To be able to write Python scripts for security applications Prerequisite: Basic knowledge of computer networks. Topic Outline: • Control systems and networks (SCADA, DCS[1], ICS[2]) • Human Machine Interfaces (HMI) • Communication Protocols: ModBus, Profibus, OPC[3], DNP3[4], EtherNet/IP[5], • Deep Packet Inspection of Control packets • Python scripting Associated Problem-based Laboratory Exercises: • Control system packet capture and analysis • Deep packet inspection • Python scripts for log analysis and reverse engineering	**Module Name**: PLC Programming and HMI Development and Security Learning Objectives: To understand the basic functions and programming of PLCs; To be able to design and implement a control system HMI; To understand HMI security. Prerequisite: Basic knowledge of control devices and associated protocols. Topic Outline: • PLC programming using Ladder Logic • Secure programming of control systems • HMI design and implementation • HMI vulnerability analysis and penetration testing Associated Problem-based Laboratory Exercises: • PLC programming • Creating a control system Human Machine Interface (HMI) (see sample HMI in Figure 1 below) • Customizing the toolkit
Module Name: Defensive Techniques and Incident Response for Control Systems Learning Objectives: To understand attack methodologies, defensive techniques and incident response for control systems. Prerequisite: Basic knowledge of computer networks, control system protocols, and security principles. Topic Outline: • Understanding basic firewall rule configuration (Authentication, Authorization, and Accounting) • Intrusion Detection and Prevention Systems on control systems • Indicators of compromise on control systems • Event investigation and data analysis	**Module Name**: Control System Vulnerability Assessment and Penetration Testing Learning Objectives: To understand control system vulnerability assessment; To be able to perform penetration testing of control systems; To be able to recommend remedial actions for control system hardening. Prerequisite: Basic knowledge of control system and network protocols. Topic Outline: • Attack surfaces of control systems • Vulnerability assessment and tools • Penetration testing and tools Associated Problem-based Laboratory Exercises:

[1] Distributed Control System
[2] Industrial Control System
[3] Object Linking and Embedding for Process Control
[4] Distributed Network Proocol 3
[5] Ethernet Industrial Protocol

• Incident response policy and plans on control systems • Evidence handling and administration Associated Problem-based Laboratory Exercises: • Configure an IDS for a control system environment • Configure and test a firewall configuration for the toolkit • Design a modular firewall policy; Critique a given firewall policy • Perform a behavioral analysis of a compromised control system	• Control system reconnaissance and mapping • Vulnerability assessment of control systems • Penetration testing of control system networks • Maintaining exploits and backdoors • Data exfiltration detection

The Embedded Systems (ES) Curriculum Modules

The following ES security curriculum modules are also designed to be self-contained: Secure Firmware Development and Embedded System Authentication. These modules are detailed in Table 2.

Table 2. The Embedded Systems Security Curriculum Modules

Module Name: Secure Firmware Development Learning Objective: To understand secure coding of firmware on embedded systems Prerequisite: Basic knowledge of computer programming. Topic Outline: • Understanding embedded systems • Secure firmware coding Associated Problem-based Laboratory Exercises: • Exploiting a firmware • Reverse engineering a firmware • Secure coding	**Module Name**: Embedded System Authentication Learning Objectives: To understand basic cryptographic techniques; To be able to design and implement lightweight encryption system for authentication; To understand the limitations of ES security. Prerequisite: Basic knowledge of discrete math and programming. Topic Outline: • Cryptography • Tiny Encryption Algorithm (TEA) • Networking fundamentals Associated Problem-based Laboratory Exercises: • Design of a basic authentication system for an embedded system • Implementation of the TEA encryption system on client and embedded system

The Guidelines, Standards, and Policy Curriculum Modules

The protection of control systems operating our nation's critical infrastructures should also include a basic understanding of the managerial, legal, and physical aspects pertinent to those systems. Thus, additional curriculum modules specific to industrial control systems security were developed and made available as supplementary materials. These modules include, but not limited to, Guidelines and Standards, Regulations and Compliance, Security Policies and Procedures, Management and Operational Controls, Risk Management, and Physical Security. The proposed modules covered the managerial, legal, regulatory, and physical aspects of critical infrastructure protection are shown in Table 3.

Table 3. Guidelines, Standards, and Policy Curriculum Modules

Module Name: National Preparedness Plan and Cyber Learning Objective: To understand the National Preparedness Guidelines in PPD-8 as it relates to cybersecurity and critical infrastructure Prerequisite: Basic knowledge of laws and regulations. Topic Outline: • Review of PPD-8 • Examination of the cybersecurity and critical infrastructure plan • Understand the laws and regulations • Case study Associated Problem-based Laboratory Exercises: • Discussion on the plan and how they can implement increased cybersecurity protocols.	Module Name: Risk, Response, Recovery, and the Command Center Learning Objectives: To understand how to assess risk to build response and recovery plans in an ICS model Prerequisite: Basic knowledge of risk response, and recovery. Topic Outline: • Defining Risk • Identifying Risk Assessment Methods • Transitioning Risk to Response and Recovery Planning • The role of Command Center in Response and Recovery Associated Problem-based Laboratory Exercises: • Scenario-based group activity will walk them through the risk assessment, framing a response and recovery plan based on the ICS model.
Module Name: Protecting Systems: Physical and Virtual Security and Policy Design Learning Objective: To understand the role of physical and virtual security rely on policy design Prerequisite: Basic knowledge of critical infrastructure and security practices. Topic Outline: • Overview of physical security methods • Review virtual security measures • Examination how policies can enhance or detract from those measures	Module Name: Managing Operations and Controls Learning Objectives: To understand techniques effective strategies in managing operations and controls Prerequisite: Basic knowledge of operations and controls. Topic Outline: • Defining operations and controls • Identifying management strategies • Change Management

Associated Problem-based Laboratory Exercises: • Conduct a SWOT analysis their current security measures and policies	Associated Problem-based Laboratory Exercises: • Building upon the SWOT analysis, participants will discuss how to implement increased protocols to provide increased security measures as it relates to operations and controls.

The Development and Implementation Processes

A subset of the course modules was used in a course titled "Embedded and Control Systems Security" in the Spring semester of 2018. The goals are to expose the students in that course to the Problem Based Learning approach and to measure the effectiveness of the learning modules.

We believe that this collection of curriculum content is appropriate for the level of expertise that we expect from the students at the CAE-2Y, CAE-CDE, CAE-R, and CAE-CO. Further, for each module, we provide multiple hands-on laboratory projects that introduces the PBL approach to learning and enable the learners to practice the technique in order to gain a better understanding of the concepts involved. To enable widespread dissemination, we provide an accompanying videocast for each module and hands-on activity and an easy access to the pedagogical materials through a website. The curriculum modules are embodied as living documents, which will be continuously enhanced and expanded in subsequent years.

The protection of control systems operating our nation's critical infrastructures should also include a basic understanding of the managerial, legal, and physical aspects pertinent to those systems. Thus, additional curriculum modules specific to industrial control systems security were developed and made available as supplementary materials. These modules include, but not limited to, Guidelines and Standards, Regulations and Compliance, Security Policies and Procedures, Management and Operational Controls, Risk Management, and Physical Security. The subjects were arranged in a natural progression from baseline processes to a complete in-depth analysis and recovery of ICS systems after an incident.

LABORATORY SETUP AND ASSOCIATED HARDWARE

To facilitate active learning, each module is accompanied by one or more laboratory activities that reinforce the concepts that were taught in the lectures. A typically computer laboratory is augmented by two very inexpensive devices: a PLC toolkit and a development board. These devices are equipped with Ethernet ports and can easily be attached to the laboratory's network switch/router. The total cost of implementing these embedded systems and industrial control system curricula modules is approximately $700: $200 for the development board and $500 for the PLC toolkit. The affordability of the accompanying hardware makes these modules appealing for widespread adoption.

The Do-more H2 Series PLC starter kit with embedded 10/100 Base-T Ethernet, as shown in Figure 1, includes an H2-DM1E CPU, a 3-slot base, an input simulator, an output module, a USB

port for programming, and a free development software. Total memory space is 262 kBytes and capable of 65K instruction words. It also includes an RS-232 port for Modbus RTU master and slave connections.

The BIG8051 Development System, shown in Figure 2, from MikroElektronika is a full-featured platform for embedded systems programming. It is based on the Silicon Labs C8051F040, a highly integrated microcontroller derived from the popular and mature Intel 8051 architecture. It features a rich variety of integrated peripheral modules, including an MMC/SD card slot, a serial Ethernet module, a USB communication interface, and numerous input and output ports. This makes the BIG8051 ideal for device prototyping, and for exploring microcontroller programming and Internet of Things applications in a classroom or laboratory environment.

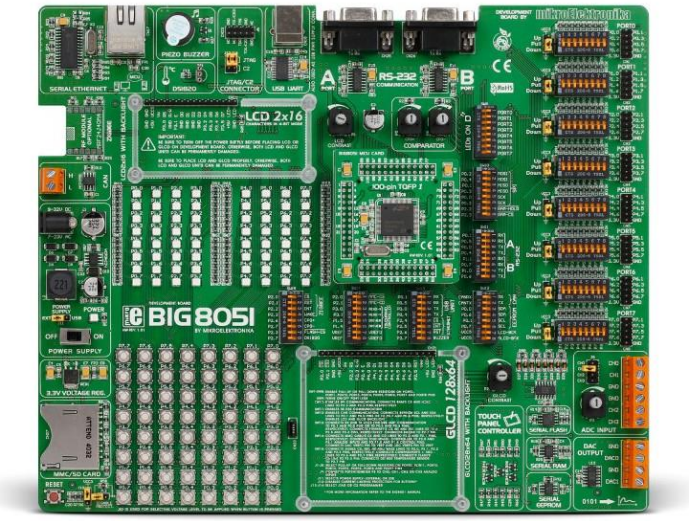

Figure 1. PLC Toolkit (Automation Direct)

Figure 2. BIG8051 Development Board (MikroElectronika)

Figure 3. The ES-ICS Security Workbench

DETAILS OF THE LABORATORY PROJECTS

The development of the hands-on exercises that were used in the ICS laboratory projects are based on the 10 curriculum modules described above.

ICS Network Protocols

Description

Industrial control system protocols range from wired to wireless. Wired protocols include Ethernet Industrial Protocol (Ethernet/IP), Common Industrial Protocol (CIP), Modbus, Modbus Transmission Control Protocol (Modbus/TCP), Distributed Network Protocol version3 (DNP3), Process Field Bus (Profibus), DeviceNet, Controller Area Network (CAN, 2013), and Ethernet for Control Automation Technology (EtherCAT). With the ever-increasing risk that ICS are being subjected to, it is imperative that cybersecurity professionals gain a good understanding of the communication protocols with which these systems operate and the threats that exist in securing them. The laboratory exercises are focused on the analysis of network packets of various ICS protocols and the development of Python-based utility tools.

Laboratory Exercises

Exercise 1: Perform a deep packet analysis of captured DNP3 network packets.

Exercise 2: Perform a deep packet analysis of captured IEC 60870-5-104 network packets.

Exercise 3: Perform a deep packet analysis of captured Ethernet/IP network packets.

Exercises 4-6: Various introductory and security-related Python programming projects.

PLC Programming and HMI Development

Description

A Programmable Logic Controller (PLC) consists of a CPU, a storage space, and input/output circuits. It is a self-contained computing device that is geared mostly for industrial control. It is programmed to realize the various functions required by industrial processes such as robot controls, equipment operations, status diagnostics, etc. The PLC instruction set may include logic, timing, counting, communication, math, input/output (I/O) control.

A Human Machine Interface (HMI) provides an intuitive interface to facilitate the interaction between the human operator and the control devices. Further, it enables effective process automation and monitoring by depicting process data and status using graphical displays.

The laboratory activities in this module provide the hands-on experiences for students to learn PLC programming using ladder logic diagram and to implement the associated HMI for each of the PLC programs.

Laboratory Exercises

Exercise 1: Implementation of a standard Up-counter in a PLC utilizing ladder logic diagram.

Exercise 2: Implementation of a 2-way light switching system for a two-storey building utilizing ladder logic diagram.

Exercise 3: Implementation of a Timer Down PLC component to realize an automatic baking oven utilizing ladder logic diagram.

Exercises 4-6: Implementation of corresponding HMIs for each of the PLC applications described in Exercises 1-3.

Defensive Techniques and Incident Response for ICS

Description

The purpose of a Cyber Security Incident Response Plan is to provide the necessary mechanism to detect and respond to cyber security incidents as well as to protect critical data, assets, and systems to prevent incidents from happening.

The concept of a firewall originated from the wall that separates sections of a building having the purpose of preventing fire from spreading from one section to another. In network security, a firewall is a device that determines whether to allow or discard a packet that goes through it depending on certain preset policies.

The lab exercises associated with this module involve analyzing and expanding a default firewall rule set, developing incident handling checklists, and configuring a Snort-base intrusion detection system that is specific to ICS. To make the firewall exercises as universally applicable as possible, we have chosen DD-WRT, an open-source firewall firmware solution which is supported by many commercial routers.

Laboratory Exercises (Firewall)

Exercise 1: Prepare the laboratory scenario by deploying an HMI application and PLC firmware. Both are designed to communicate using the Modbus/TCP protocol; in this lab, they are used to test Modbus/TCP connectivity within and between local area networks.

Exercise 2: Prepare a commercial router for use with control systems networks. This includes: enabling secure shell access for remote management and enabling logging.

Exercise 3: Prepare the lab workstation for subsequent activities. If the workstation is not already equipped with a secure shell (SSH) client, this lab exercise guides the participant through the installation and configuration of the client and concludes by testing connectivity with the secure shell server in the router.

Exercise 4: Configure the firewall. After critiquing the default firewall configuration, the participant is guided through the implementation of several layered firewall policies. These range from open Modbus/TCP access to more restricted access; at each stage, Modbus/TCP connectivity is tested between the HMI, PLC, and the lab workstations. Finally, the participant is guided through the process of monitoring the firewall, checking the firewall logs, and permanently committing the completed and tested firewall policy.

Laboratory Exercises (Incident Response)

Exercise 1: Develop an incident handling checklist similar to the Generalized Incident Handling checklist in NIST SP 800-61r2 that is specific to a Data Exfiltration incident. Describe the purpose of each checklist item.

Exercise 2: Develop an incident handling checklist similar to the Generalized Incident Handling checklist in NIST SP 800-61r2 that is specific to a Malicious Code incident. Describe the purpose of each checklist item.

Laboratory Exercises (Intrusion Detection System)

Exercise 1: Deploy an IDS for a Modbus device that will monitor critical activities in a Modbus protocol system.

Control System Vulnerability Assessment and Penetration Testing

Description

Vulnerability assessment (VA) is the process of identifying, documenting, and analyzing the vulnerabilities of a system. This process yields a list of vulnerabilities which are prioritized based on their criticality to impact the business objectives of the enterprise. Further, the results of this process, including the remediation steps taken to resolve the discovered vulnerabilities, can often be used to satisfy certain regulatory audit or compliance requirements.

ICS network reconnaissance is the process of scanning the network for the purpose of discovering the ICS devices attached to the network and their vital characteristics such ports opened and closed, IP addresses, services offered, and operating systems. Although this process seems to be passive and non-intrusive, it could have a harmful effect on an ICS.

Penetration testing is the process of testing a system, network, web interfaces, or applications with the intent of discovering vulnerabilities that an adversary may be able to exploit. The process can be performed manually, automated with software tools, or carried out using a technique that combines both. In some sense, penetration testing is a simulated adversarial attack.

Laboratory Exercises

Exercises 1 & 2: Perform scanning and enumeration techniques utilizing Zenmap to discover control devices on an internal network. Perform a system reconnaissance using Zenmap and Shodan to discover PLC devices on the local network and on the Internet, respectively.

Exercise 3: Perform vulnerability assessment of a control device on the internal network utilizing OpenVas and generate a detailed report of the discovered vulnerabilities.

Exercises 4 & 5: Utilizing Kali Linux, Metasploit, Armitage, and Modbusclient, exploit an HMI device with an attack originating from the external network.

Secure Firmware Development

Description

Secure Firmware Development explores embedded systems from a programming perspective, with an emphasis on secure applications. Starting with an introduction to embedded systems in general, and microcontrollers in particular, it proceeds to explore the various applications of embedded systems, and the unique challenges faced by embedded system designers. The labs introduce the participant to embedded system development tools and presents hands-on exercises which include the use of an in-circuit debugger for real-time memory inspection and troubleshooting. The module concludes with a detailed discussion of secure coding standards and defensive programming practices and presents the participant with the challenge of applying these practices to resolve a security-related flaw in an example embedded system.

Laboratory Exercises

Exercise 1: Install and configure the suite of microcontroller development tools provided by Silicon Labs and configure the BIG8051 Development System for first-time use.

Exercise 2: Use the in-circuit debugger, and the memory inspection tools of the Silicon Labs IDE, to control and monitor a firmware program during execution. Activities include single-stepping through program instructions, viewing and modifying the contents of memory during program execution, and programming the microcontroller's input/output ports.

Exercise 3: Apply the defensive programming ideas discussed in the lessons to discover and repair a security-related flaw. The participants are given a precompiled firmware binary for a complete embedded system which deliberately includes a serious security flaw. In Part One, the participants must discover a consistent exploit for this flaw using black-box testing techniques, and in Part Two, the participants are given the source code and must reverse-engineer it, using the debugging tools and the programming practices discussed earlier. Once the participants have identified the source of the security flaw and the reasons the flaw has the effect that it does in the system, they are asked to resolve the flaw, without affecting the functionality of the system.

Embedded System Authentication

Description

Embedded System Authentication explores the application of cryptographic techniques to embedded systems. It begins with an introduction to cryptography, the major applications of cryptographic algorithms, and the characteristics of strong cryptosystems. It then discusses the various problems of implementing strong cryptography within the constraints of embedded systems, and presents one cryptographic algorithm, the Tiny Encryption Algorithm (TEA), as an ideal example of small and efficient embedded systems programming which nonetheless provides a reasonable level of protection. It then introduces the user to the Java programming language and platform, exploring input/output in Java and the use of the RXTX communication libraries for data exchange with embedded systems.

Laboratory Exercises

Exercise 1: An entry-level exercise, intended to introduce the use of serial ports and serial networks for embedded system communications. This exercise involves configuring the BIG8051 Development System to enable data exchange with the PC; this involves using the virtual serial port on the BIG8051, and the Java Development Kit (JDK) and the RXTX communication libraries on the PC.

Exercise 2: Explore lightweight cryptography for embedded systems by implementing the Tiny Encryption Algorithm (TEA) on two platforms: on the microcontroller platform using C, and on the PC platform using Java. The participant is challenged to use this algorithm to implement secure communications between the two platforms, encrypting on one platform and decrypting on the other.

Exercise 3: Expand the encryption algorithm implementation completed in the previous lab to add the ability to encrypt and decrypt eight-byte alphanumeric blocks. Again, the participant must implement the algorithm on both platforms; in the process, the participant explores such cross-platform development issues as integer precision and bitwise manipulation of signed numbers.

Exercise 4: The final exercise explores the security of lightweight cryptography by staging a brute-force attack on the TEA algorithm. Using the encryption tools developed in the earlier labs, the participant is presented with a brute-force password cracking tool (or is asked to develop this tool themselves, at the instructor's discretion), and is challenged to crack the encryption using keys of varying degrees of complexity.

National Preparedness Plan and Cyber

Description

The *National Preparedness Plan and Cyber* modules introduced and expanded the participants understanding of policy-decisions and government role in protecting the critical infrastructure and cyberspace. Few are aware that Presidential Policy Directive-8 (Obama, 2015) known as the National Preparedness Plan includes cybersecurity in addition to natural and other man-made disasters.

Laboratory Exercises

Exercise 1: Cyber Hygiene Kit introduced a connection between the *Blueprint for a Secure Cyber Future* (2011) and the protection of the critical infrastructure. Participants in this lab are asked to evaluate their level of protection and maintenance on their home systems. The checklist will verify the number of systems, peripheral devices, authorized users, maintenance schedule, and patch levels to ensure the system is properly maintained and protected. Then participants are asked to reflect on how the practice on their systems at home translates to the CI and ICS practices.

Exercise 2: Participants are asked to read the *Electric Power Generation and Transmission: Creating a Sustainable NERC CIP Compliance Program* (Lockheed Martin, 2014) Case Study with a software solution and *Cyber security of power grid: State-of-the-Art* (Sun, Hahn, and Liu, 2018), which reviews "(1) a survey of the state-of-the-art smart grid technologies, (2) power industry practices and standards, (3) solutions that address cyber security issues, (4) a review of existing CPS testbeds for cyber security research, and (5) unsolved cyber security problems. Based on the review of the laws, presidential directives, regulations, and policies, participants will be asked to compare the information in the article concerning unsolved cyber security problems to identify best practices that could be used to detect and deter attacks against the power grid.

Protecting Systems: Physical and Virtual Security and Policy Design

Description

The *Protecting Systems: Physical and Virtual Security and Policy Design* module has participants explore the steps of physical and cyber vulnerability threat assessments. A discussion on the information obtained in the vulnerability threat assessments can be used to create, enhance, or remove policy. Participants are asked to retain their lab information for future labs.

Laboratory Exercises

Exercise 1: In this lab, participants will assess the potential hazards at their workplace. The identified hazards will be categorized as low, moderate, and high according to impact and probability. Participants are given websites containing statistics on Active Shooters, Hazardous Waste Contamination, Hurricanes, Power Outages, Tornadoes and Wildfires to determine the probability in their area. In addition to the natural and man-made disasters, participants are asked to speak to their systems administrator or Information Technology Staff to determine the number of malware attacks, denial of service, and other intrusions. This information will provide insight to events that have the highest impact and probability, which should be addressed first. This information is used in future modules to create Cyber Incident Risk Assessment, CIRT Response and IT Disaster Recovery Plan, and Post-Incident Handling lab.

Exercise 2: The Self-Assessments: Vulnerability Management ask participants to identify the vulnerabilities on their home system. The areas to be reviewed include the tools used to identify vulnerabilities such as scheduled patching for systems, updated software applications, ability to detect malicious code on home systems and mobile devices. Participants will be asked to list the identified vulnerabilities, categorize and prioritize the vulnerability, determine if the vulnerability is actively discovered, and the relevance of the vulnerability to their home system. Maintaining a list of vulnerabilities and actions is recommended.

Exercise 3: Conduct a second SWOT analysis using the materials discussed in the entitled article: *Transforming Power Operations and Maintenance Efficiency with Advanced Asset Information Management* (Smith, 2018). Identify and list additional or modified best practices to add to your organization based on the content in the article and content within this module.

Risk, Response, Recovery and the Command Center

Description

Risk Management, Response, Recovery, and the Command Center is predicated on the content and labs from Modules 7 and 8. To effectively determine risk, response, recovery, and command center operations, the identification of mitigating circumstances is paramount. The first five labs are the assessment steps in the cyber incident risk management (CIRM) plan. The confluence of data from physical and virtual vulnerability threat assessments, All Hazards Models, and Cyber Incident Risk Management coalesces into a comprehensive IT Disaster Recovery, cyber incident response, and unified Command Center. At the end of Module 9, participants in the final assessment and lab combination will be engaged in a decision-tree cyber incident scenario to test their understanding on how to respond to a cyberattack. The first five lab exercises will walk participants through a cyber incident risk management assessment to build a plan.

Laboratory Exercises

Exercise 1: Participants are asked to conduct a cyber risk assessment worksheet will identify potential risks at either their workplace or home systems.

Exercise 2: The Risk Impact Scale is the next step to rank the identified issues in Lab 1 based on severity and area of risk. This process teaches the participants how to prioritize risk based on the mission, strategies, financial, regulatory and compliance guidelines.

Exercise 3: The Opportunity Impact Scale will convey to participants that some risks can present opportunities. Participants will need to determine out of the identified areas of risk and what opportunities if any are present within that identified area.

Exercise 4: Likelihood Scale Lab instruct the participants to rank the possibility of occurrence based on the identified areas of risk and/or opportunity. To score the risk or opportunity, participants consider the impact and probability based on low, low-medium, medium, medium-high, and high for both categories. Once a decision is made, the item is plotted on the chart.

Exercise 5: Risk/Opportunity Evaluation and Response Lab will have participants determine the Risk/Opportunity Response Strategy**,** Response Plan**,** Cost Estimate**,** Other Resources Needed**,** and the Target Completion Date. This is the last step to determine which risks and opportunities will be addressed based on priority, the timeframe of resolution, the resolution, and by whom the risk/opportunity will be addressed.

Exercise 6: The Cyber Scenario is the final lab for Module 9 will be a decision tree cyber scenario that uses a cyberattack method discussed in the module. Based on the information the participants have been given in this module and other external resources, the participants will have to decide the type of attack, and the correct order of handling the incident before power is restored to the region. Participants will use a variety of techniques such as multiple choice to drag and drop to determine the best method of solving the incident. Once the scenario is completed, participants are asked to print a copy of their scenario. This information will then be used to complete the Capstone at the end of Module 10.

Managing Operations and Controls

Description

Although managing operations, controls, and compliance are a daily operational task, these areas are critical during a post-incident. The recovery from a cyberattack and restoring compliance and regulatory standards is a process. Therefore, participants are asked to conduct labs and assessments to regain regulatory and compliance standards with minimal impact to the organization.

Laboratory Exercises

Exercise 1: ICS Systems lab asks participants to search the internet to find consumer products that are or could be classified as Supervisory Control and Data Acquisition (SCADA), Distributed Control Systems (DCS), and Process Control Systems (PCS).

Exercise 2: Participants will search the internet to find cyber laws that are associated with Industrial Control Systems and/or the critical infrastructure. This lab will demonstrate the number of laws and regulations that are in place to protect ICS and CI.

Exercise 3: Participants are also asked to review the 10 Self-Assessment domains in the Cyber Resilience Review (CRR) to determine if the primary role of the domain is under managing operations, controls, or compliance and give explanations for their decision. This exercise will demonstrate the purpose of CRR and how that framework guides or governs the actions of ICS and CIP.

Exercise 4: The participants' last lab is a capstone, which refers back to the cyber scenario in Module 9. In the capstone, the participants will be asked to identify from prior assessments and labs the areas where their organization could permit such an attack at their location. Then the participants will determine which laws, policies, regulations, and compliance standards have been violated. The final step is an action plan or post-incident handling plan on how the organization can regain their "good standing" with the laws, regulations, operations, and compliance guidelines that were breached or violated during the attack.

LAB ASSESSMENTS

The labs were created with supporting documentation and examples to demonstrate the correct protocol or processes. Content assessments were included throughout the modules to confirm the participants' level of understanding in the information given. For instance, to gauge the effectiveness of the materials used in the Embedded System Security and Industrial Control System Security curriculum modules, the lessons and laboratory exercises were piloted in two sections of an Embedded and Control Systems Security course during the Spring 2018 semester.

Two pilot surveys were given to the students in both sections. The first survey was distributed at the beginning of the semester, a total of 36 students (n=36) participated. The second survey was given upon completion of the course. The post-survey had 35 students (n=35) participate. Although the students that participated in the pre-survey were to take the post-survey, the pilot research design was disrupted. In Spring, 2018 an EF3 tornado struck the university campus and the greater community area. Due to this unusual event occurring close to the close of the Spring Semester, students were provided completion options that included (1) complete the

course, (2) accept the current grade, or (3) receive an Incomplete. Therefore, the pilot pre- and post-surveys will be redistributed in future semesters to establish reliability and validity.

The six questions on the pre-semester survey were as follows:

1. Rate your own level of experience with project-oriented microcontroller kits, such as the Arduino.
2. Rate your own level of experience with Programmable Logic Controllers (PLCs), such as those used in Industrial Control Systems.
3. What is your present level of experience with using ladder logic to develop firmware for Programmable Logic Controllers (PLCs)?
4. What is your present level of experience with using human machine interface (HMI) tools to develop applications for monitoring and controlling Programmable Logic Controllers (PLCs)?
5. How would you rate your present level of awareness of Control Systems Security issues?
6. How would you rate your present level of awareness of Embedded Systems Security issues?

The corresponding six questions on the post-semester survey included:

1. How would you rate your new level of understanding of microcontrollers and microcontroller programming?
2. How would you rate your new level of understanding of Programmable Logic Controllers (PLCs)?
3. How would you rate your new level of understanding of ladder logic programming?
4. How would you rate your new level of understanding of human machine interface (HMI) programming?
5. How would you rate your new level of awareness of Control Systems Security issues?
6. How would you rate your new level of awareness of Embedded Systems Security issues?

The pre-semester survey questions were designed to assess: (1) the students' previous experience with embedded systems, (2) their level of awareness of embedded systems security issues, and (3) establish a baseline of measure to compare the post-semester survey. When the post-semester survey was distributed, students were asked if the work in the course had increased or decreased their level of interest in pursuing further study of embedded systems by selecting the indicator that best described their level of agreement:

- "My experience in this class has made me more comfortable with the idea of working with embedded systems (including microcontrollers and PLCs) as development platforms."
- "My experience in this class has made me more interested in pursuing projects which make use of embedded systems, either as a career or for personal enjoyment."
- "My experience in this class has helped me to better understand the role of embedded systems in everyday life, including their use in devices that I regularly use or rely on."

- "My experience in this class has helped me to better understand the security-related challenges of embedded systems design."
- "My experience in this class has helped me to better understand the approaches and tools that programmers can take to solving the aforementioned security problems."

In addition to the questions listed above, students were asked to rate the following on a 1 to 10 scale and the findings are displayed in Table1.1 Pre-and Post-Semester Assessment Results. The four areas students were asked to rank included:

- The effectiveness of the course materials
- The development tools and equipment used in the course
- Their own confidence in undertaking ES-ICS security activities
- How much the course increased or decreased their interest in information security in general, and embedded systems security in particular

Table1.1 Pre-and Post-Semester Assessment Results

Question/Response Options	**Pre-** (*n*=36)	**Post-** (*n*=35)
Question 1 Rate your level of understanding (or experience) of microcontrollers and microcontroller programming.		
• I never used them/Very Unfamiliar	83.33%	0%
• I've used them only once or twice/Somewhat Unfamiliar	16.67%	2.86%
• I've used them occasionally/Somewhat Familiar	0%	57.14%
• I've used them extensively/Very Familiar	0%	40%
Question 2 Rate your level of understanding (or experience) with Programmable Logic Controllers (PLCs).		
• I never used them/Very Unfamiliar	88.89%	0
• I've used them only once or twice/Somewhat Unfamiliar	11.11%	2.86%
• I've used them occasionally/Somewhat Familiar	0%	60%
• I've used them extensively/Very Familiar	0%	37.14%
Question 3 Rate your level of understanding (or experience) with ladder logic programming.		
• I never used them/Very Unfamiliar	88.89%	0%
• I've used them only once or twice/Somewhat Unfamiliar	11.11%	11.43%
• I've used them occasionally/Somewhat Familiar	0%	57.14%
• I've used them extensively/Very Familiar	0%	14.29%
• N/A (did not participate due to the tornado)		17.14%
Question 4 Rate your level of understanding (or experience) with HMI programming.		
• I never used them/Very Unfamiliar	88.89%	0%
• I've used them only once or twice/Somewhat Unfamiliar	11.11%	11.43%
• I've used them occasionally/Somewhat Familiar	0%	57.14%
• I've used them extensively/Very Familiar	0%	14.29%
• N/A (did not participate due to the tornado)		17.14%
Question 5 What is your present level of awareness of Control Systems Security issues?		
• I never used them/Very Unfamiliar	50%	0%
• I've used them only once or twice/Somewhat Unfamiliar	30.56%	5.72%

• I've used them occasionally/Somewhat Familiar	19.44%	45.71%
• I've used them extensively/Very Familiar	0%	48.57%
Question 6		
What is your present level of awareness of Embedded Systems Security issues?		
• I never used them/Very Unfamiliar	55.56%	0%
• I've used them only once or twice/Somewhat Unfamiliar	30.55%	8.57%
• I've used them occasionally/Somewhat Familiar	13.89%	40%
• I've used them extensively/Very Familiar	0%	51.43%

The summary of the post-semester assessment findings is shown in Table 1.2.

Table 1.2 Post-Semester Assessment Results

Questions	**Results (*n*=35)**	
My experience in this class has made me more comfortable with the idea of working with embedded systems (including microcontrollers and PLCs) as development platforms.	Strongly disagree: Somewhat disagree: Somewhat agree: Agree: Strongly agree:	0% 2.86% 8.57% 45.71% 42.86%
My experience in this class has made me more interested in pursuing projects which make use of embedded systems, either as a career or for personal enjoyment.	Strongly disagree: Somewhat disagree: Somewhat agree: Agree: Strongly agree:	0% 5.71% 11.43% 48.57% 34.29%
My experience in this class has helped me to better understand the role of embedded systems in everyday life, including their use in devices that I regularly use or rely on.	Strongly disagree: Somewhat disagree: Somewhat agree: Agree: Strongly agree:	0% 0% 5.72% 25.71% 68.57%
My experience in this class has helped me to better understand the security-related challenges of embedded systems design.	Strongly disagree: Somewhat disagree: Somewhat agree: Agree: Strongly agree:	0% 0% 2.86% 40% 57.14%
My experience in this class has helped me to better understand the approaches and tools that programmers can take to solving the aforementioned security problems.	Strongly disagree: Somewhat disagree: Somewhat agree: Agree: Strongly agree:	0% 2.86% 11.43% 45.71% 40%
On a scale of 1 to 10 (in which 10 is "very confident" and 1 is "no confidence at all"), rate your confidence in undertaking Embedded Systems and Industrial Control Systems (ES-ICS) security activities.	10 (very confident): 9: 8: 7: 6: 5: 4: 3: 2: 1 (no confidence at all):	0 5 11 10 3 5 1 0 0 0
On a scale of 1 to 10 (in which 10 is "very effective" and 1 is "not effective at all"), rate the effectiveness of the course materials used in learning about ES-ICS security.	10 (very effective): 9: 8: 7:	15 7 7 3

	6:	1
	5:	1
	4:	0
	3:	0
	2:	0
	1 (not effective at all):	0
On a scale of 1 to 10 (in which 10 is "very effective" and 1 is "not effective at all"), rate the effectiveness of the tools used in learning about ES-ICS security.	10 (very effective):	17
	9:	6
	8:	8
	7:	3
	6:	1
	5:	0
	4:	0
	3:	0
	2:	0
	1 (not effective at all):	0
On a scale of 1 to 10 (in which 10 is "greatest increase", 5 is "neutral", and 1 is "greatest decrease"), rate how much the course increased or decreased your interest in ES-ICS security, or Information Security in general.	10 (greatest increase):	9
	9:	5
	8:	10
	7:	4
	6:	2
	5 (neutral):	5
	4:	0
	3:	0
	2:	0
	1 (greatest decrease):	0

The assessments for embedded systems, the modules contained additional assessments to gauge the participant's understanding of the content. The lab assignments can connect to a database or learning management system (LMS) to track the participants' progression, which would allow further analysis. The culmination of surveys, successful completion of the labs, and assessments in the module are validate the effectiveness of the module content and the accompanying laboratory exercises.

CONCLUSION AND FUTURE PLANS

In this paper, we presented the design and implementation of Embedded Systems (ES) and Industrial Control Systems (ICS) security curriculum modules. We also described the laboratory setup and the associated hands-on exercises that are pertinent to each module. We believe that the problem-based approach to learning is enhanced by the carefully designed activities that accompany the lecture modules. The capstone exercise on applying the various laws, policies, regulations, and compliance standards to specific attack scenarios provide a realistic table-top exercise for participants to be able to apply their newly acquired knowledge on ICS security and Critical Infrastructure Protection.

Future plans, connected with these curriculum modules and activities, are the following:

- The continuous evaluation of the effectiveness of the curriculum modules and laboratory exercises;
- The enhancement of the table-top exercises with additional real-world scenarios; and

- The development of additional curriculum modules in the areas of threat intelligence, machine learning, indicators of compromise, and attack attribution pertaining to ICS and ES security.

REFERENCES

Brookfield, S. (1995). Adult learning: An overview. In A. Tuinjman (Ed.), International Encyclopedia of Education. Oxford, Pergamon Press.

Champion, R. (2003). Taking measure: The real measure of professional development program's effectiveness lies in what participants learned. Journal of Staff Development, 24(1), 1–5.

Creswell, J. (2005). Education Research: planning, conducting, and evaluating quantitative and qualitative research (2nd ed.) Upper Saddle River, NJ: Merrill.

Cyber Security Education Consortium (CSEC) (2014). CSEC Advances Cybersecurity & Homeland Defense. Website: https://atecenters.org/st/csec/. Accessed: August 10, 2018.

U.S. Department of Energy (DOE), (2015). Office of Electricity Delivery and Energy Reliability, "Energy Sector Cybersecurity Framework Implementation Guidance." January, 2015. Website: http://www.energy.gov/sites/prod/files/2015/01/f19/Energy%20Sector%20Cybersecurity%20Framework%20Implementation%20Guidance_FINAL_01-05-15.pdf. Accessed: August 10, 2018.

Francia, G. A., Bekhouche, N., Marbut, T. M., & Neuman, C. (2012). Portable SCADA Security Toolkits. International Journal of Information & Network Security (IJINS), 1(4), 265-274.

Francia, G. A. & Francia, X. P. (2014). Critical Infrastructure Protection and Security Benchmarks. In M. Khrosrow-Pour (Ed.), Encyclopedia of Information Science and Technology, 3rd Ed (3rd ed., pp. 4267-4278). Hershey, PA: IGI-Global Publishing.

Francia, G. A., & Snellen, J. (2014). Embedded and Control Systems Security Projects. Information Security Education Journal (ISEJ), Vol. 1, no. 2, pp. 77-84, December, 2014.

Francia, G.A., Randall, G., & Snellen, J., "Pedagogical Resources for Industrial Control Systems Security: Design, Implementation, Conveyance, and Evaluation," Journal of Cybersecurity Education, Research and Practice: Vol. 2016, No. 4. Available at: https://digitalcommons.kennesaw.edu/ccerp/2016/Academic/4/

Francia, G.A., Francia, X.P., & Pruitt, A.M., "Towards an In-depth Understanding of Deep Packet Inspection Using a Suite of Industrial Control Systems Protocol Packets," Journal of Cybersecurity Education, Research and Practice: Vol. 2016, No. 2, Article 2. Available at: http://digitalcommons.kennesaw.edu/jcerp/vol2016/iss2/2

Fulton, K., & Britton, T. (2011). STEM teachers in professional learning communities: From good teachers to great teaching. Washington, DC: National Commission on Teaching and America's Future. Retrieved from http://www.eric.ed.gov/PDFS/ED521328.pdf

Ganzer, T. (Ed.) (2000). Ambitious visions of professional development for teachers [Special Issue]. National Association for Secondary School Principals, (84)618.

Glattenhorn, A. (1987). Cooperative professional development: Peer centered options for teacher growth. Educational Leadership, (3)45, 31-35.

Hung, W., Jonassen, D. H., & Liu, R. (2008). Problem-based learning. In J. M. Spector, J. G. van Merriënboer, M. D., Merrill, & M. Driscoll (Eds.), Handbook of research on educational communications and technology (3rd ed., pp. 485-506). Mahwah, NJ: Erlbaum.

Idaho National Laboratory (INL) (2014). National SCADA Test Bed Program. Website: http://www.inl.gov/scada/. Accessed: November 8, 2015.

Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) (2015). "Incident Response/Vulnerability Coordination in 2014." ICS-CERT Monitor. September, 2014-February, 2015. Website: https://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Sep2014-Feb2015.pdf.

Lieb, S. (1991). Principles of adult learning. Honolulu Community College. Retrieved July 01, 2016, from http://design2learn.ch/downloads/principles_of_adult_learning_lieb.pdf

Lockheed Martin. (2014, October). Electric Power Generation & Transmission Creating a Sustainable NERC CIP Compliance Program. PennEnergy White Papers. Retrieved July 27, 2018.

National Institute of Standards and Technology (NIST), (2014) "Framework for Improving Critical Infrastructure Cybersecurity." February 12, 2014. Website: http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf. Accessed: March 30, 2016.

Nieles, M., Dempsey, Kelley, & Pillitteri, V. Y. (2017, June). NIST Special Publication 800-12 Revision 1. Retrieved August 7, 2018, from National Institute of Standards and Technology: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-12r1.pdf.

North American Electric Reliability Corporation (NERC), (2015), "Critical Infrastructure Protection (CIP) Standards." Website: http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx. Accessed: April 06, 2016.

Patton, M. (2002). Qualitative evaluation and research methods (4th ed.). Newbury Park, CA: Sage.

SANS (2014). ICS410: ICS/SCADA Security Essentials. Website: http://www.sans.org/course/ics-scada-cyber-security-essentials. Access date: November 05, 2015.

Smith, C. (2018, June). Transforming Power Operations and Maintenance Efficiency with Advanced Asset Information Management. Bentley White Paper, 1-8. Retrieved July 27, 2018.

Solomon, Howard, "Over 90 percent of ICS devices exposed to Internet are vulnerable, says Kaspersky". IT World Canada, July 11, 2016. URL: https://www.itworldcanada.com/article/over-90-per-cent-of-ics-devices-exposed-to-internet-are-vulnerable-says-kaspersky/384856.

Sun, C., Hahn, A., & Liu, C. (2018). Cyber security of a power grid: State-of-the-art. International Journal of Electrical Power & Energy Systems, 99, 45-56. doi:10.1016/j.ijepes.2017.12.020

Thornton, D. C., Francia, G. A., & Brookshire, T. (2012). Cyberattacks on SCADA Systems. (pp.9-14). Proceedings of the 16th Colloquium for Information Systems Security Education. Lake Buena Vista, FL, June 11-13, 2012. (Best Paper in CISSE Conference Award).