VOLUME 36, NUMBER 2

April-June 2020

Article
Page 2

References
Page 16

Authors

Dr. Faruk Yildiz
Associate Professor in the Department of Engineering Technology at Sam Houston State University

Dr. Recayi Pecen
Quanta Endowed Professor of Engineering Technology in the College of Science and Engineering Technology at Sam Houston State University

Dr. Ulan Dakeev
Assistant Professor of Engineering Technology in the College of Science and Engineering Technology at Sam Houston State University

The Journal of Technology, Management, and Applied Engineering© is an official publication of the Association of Technology, Management, and Applied Engineering, Copyright 2020

ATMAE
701 Exposition Place
Suite 206
Raleigh, NC 27615

www. atmae.org

JTMAE
The Journal of Technology, Management, and Applied Engineering

Educational Mobile Laboratory Unit Implementation to Study and Research Industrial Control System Vulnerabilities to Cyber Attacks

Keywords:
Automation and Control; Information Security; Digital Forensics; Cybersecurity

SUBMITTED FOR *PEER – REFEREED*

Educational Mobile Laboratory Unit Implementation to Study and Research Industrial Control System Vulnerabilities to Cyber Attacks

Dr. Faruk Yildiz is an Associate Professor in the Department of Engineering Technology at Sam Houston State University. His primary teaching areas include electronics & computer engineering technology, engineering design, and alternative energy systems. His research interests include low-power energy harvesting, conversion, and storage systems, renewable energy technologies, automation & control, STEM education. Dr. Yildiz has published and/or presented about 160 times in a variety of scholarly mediums including refereed journal articles, refereed presentations, invited workshops, teaching-related publications, and local presentations.

ABSTRACT

Supervisory Control and Data Acquisition (SCADA) is a part of Industrial Control Systems (ICS) and a prevalent control system architecture that is commonly used for industrial automation. The SCADA systems play an integral role in large-scale processes for interfacing with transducers and machinery for real-time control and data acquisition. The increasing demand to integrate SCADA systems with remote networks and the Internet of Things (IoT) technologies raises concerns for information security specialists. These systems are known to have notable security vulnerabilities and may be subject to an increasing number of cyber threats. This research work provides educational guidance on how to build and further study ICS, including SCADA systems in academia. The mobile system introduced in this paper allows researchers to further investigate cybersecurity analysis of the ICS components. There exists a need and demand to better understand these systems and the inherent security threats that come with them. The details including system infrastructure, challenges faced during the establishment of the laboratory setup, student and faculty involvement, laboratory course objectives, student assessments, and industry support are reported in the paper.

INTRODUCTION

Industrial Control Systems (ICS) are critical assets to our nation as they interact with physical aspects of our daily life. These systems often run 24/7 to control and monitor critical industrial and infrastructure processes. The demand to integrate them with the Internet has opened them up to cyber-attacks (Scheffer, Wibberley, & Beets, 2002; Velankar & Mehta, 2002). Supervisory Control and Data Acquisition (SCADA) is commonly used in the ICS to remotely gather data in real-time and allows automation and communication with networked equipment, such as Programmable Logic Controllers (PLC's). These types of systems are often seen in frameworks that require industrial automation including power plants, oil and gas refining, telecommunications, transportation, water treatment and waste control (Rouse, 2005). While SCADA systems are widely used throughout industrial automation, such systems are known to have notable security vulnerabilities and may be subject to an increasing number of cyber threats (Ahmed, Obermeier, Naedele, & Richard, 2012; Goldman, 2013; Sanger & Schmitt, 2012; Cárdenas, Amin, Huang, Huang, & Sastry, 2011; Luiifj, 2012).

SCADA systems are used to control dispersed assets where centralized data acquisition is as important as control (Morris, et al., 2011; Nguyen, Tran, & Besanger, 2016). A SCADA system generally consists of the following components: one or more distributed field sites consisting of remote terminal units and programmable logic controllers that control actuators and monitor sensors, supervisory computers/servers, a human-machine interface, alarm system, data historian, and a network infrastructure. The network infrastructure of a SCADA system is not exclusive to a single topology and can be distributed across a number of networks. To enable cross-communication between network topologies, hardware solutions such as protocol converters can be implemented. Additionally, software such as open platform communications (OPC) aim to provide interoperability by enabling communication of real-time data between devices from different manufacturers (Stouffer, Falco & Kent; 2007). SCADA communication protocols often prioritize fast transmission times and low latency. Anecdotally, this may contribute to the widespread use of legacy protocols and proprietary communications that is seen throughout the SCADA industry. SCADA systems may also have connectivity to entities outside of the SCADA network, such as a corporate network. When interconnectivity between networks is in place, a common practice is to isolate the SCADA network by implementing a firewall. Lastly, the current fourth generation SCADA architecture is defined by its increasing support for IoT technologies as a means of improving interoperability.

Dr. Recayi Pecen is serving as a Quanta Endowed Professor of Engineering Technology in the College of Science and Engineering Technology at Sam Houston State University. He served as a president and professor at North American University (NAU) at Stafford, TX from July 1, 2012 to December 12, 2016; also served as professor and program chairs of Electrical Eng. Technology and Graduate Programs in the Department of Technology at the University of Northern Iowa (UNI) between 1998 and 2012. Dr. Pecen holds a B.S. in EE and an M.S. in Controls and Computer Eng. from Istanbul Technical University, an M.S. in EE from the Univ. of Colorado at Boulder, and a Ph.D. in EE from the Univ. of Wyoming (UW, 1997). He is a senior member of IEEE, IEEE-PES, member of ASEE, Tau Beta Pi National Engineering Honor Society. Dr Pecen completed FBI Houston Citizens Leadership Academy Program in 2015-16. He successfully completed Fort Bend County Chamber of Commerce Leadership Forum for the class of 2016-17. Dr. Pecen is a recipient of 2010 Diversity Matters Award at UNI for his efforts on promoting diversity and international education. He is also a recipient of 2011 UNI C.A.R.E Sustainability Award for the recognition of applied research and development of renewable energy applications in Iowa. Dr. Pecen was recognized by Iowa Senate on June 22, 2012 for his service to state of Iowa for development of clean and renewable energy and promoting diversity and international education between 1998-2012.

According to Valli (2009), there is a lack of protection for protocols used in SCADA/ICS systems that are used all over the world for highly important operations that if forcibly or maliciously stopped could result in major economic destruction or human death.

As these systems get larger, there is a need to expand the current private local networks that they run on. As the systems expand to different locations the network has to break up, which means there are multiple networks being connected. The solution to this issue is to network them via the Internet. Connecting the networks via internet allows for Human Machine Interface (HMI) and other device access in remote areas. However, once connected to the Internet, the system may become vulnerable to hacker attacks in the ICS hardware and software components.

There are a variety of resources and subsystems for SCADA and its security systems such as the supervisory system, PLCs, HMIs, remote terminal units (RTU), communication infrastructure and instrumentation. Specifically, the vulnerabilities to cyber-attacks of automation systems when connected to the Internet have been studied. Johnson, Harkness, & Evangelopoulou made a SCADA lab that mimics real-world systems as closely as possible to test them for cybersecurity vulnerabilities (Johnson, Harkness, & Evangelopoulou, 2016). They found that very little research had been done on cybersecurity related to SCADA protocols and forensics in an industrial setting. A sample manufacturing company called "KAT Engineering and Chemicals" was created in the HMI software with random values for many of the processes. In certain situations, the lab would cause a theoretical environmental disaster. Blue and red teams would play against each other in the SCADA lab; one trying to hack into the network and disrupt processes while the other team tried to prevent it and/or figure out where the vulnerabilities were originated from. The lab was designed to allow its users to learn and comprehend the vulnerabilities in SCADA systems and remained simple upon scaling up or down depending on the cases.

A forensic toolkit was proposed based on an earlier forensic methodology for SCADA systems proposed by Stirland et al (Stirland, Jones, Janicke, & Wu, 2014). The toolkit would require hardware write blockers, a firewire PCI Card, an HD camera, as well as software bespoke PLC flashing software, FTK imager, EnCase, Helix, TCPDump, a Data hashing tool, and a text editor. The toolkit would be used to conduct each phase of the forensic methodology. Forensic methodology phases included: identification and preparation; identifying data sources; preservation, prioritizing, and collection; examination and analysis; and reporting and presentation. Another research study was conducted to study indoor SCADA systems with solar PhotoVoltaics (PV) panels used as the input field devices (Akelian, 2015).

Attacks on SCADA systems are becoming increasingly popular in conjunction with connecting the systems to wider networks. A forensic analysis is necessary to determine how to protect these systems against attacks, without interfering with the always-on nature of most SCADA systems. The amount of data a SCADA system uses is approximately 400 GB per day. If a monitoring and logging system is to be placed, it should be able to handle that amount of data without interrupting the normal flow of the SCADA system. Most SCADA systems run on old platforms that require legacy support, leading to the challenge of finding forensic software that is up to date but also runs on these really old systems. A lot of data is also volatile and changes frequently, so the forensics must have the ability read the data as fast as possible before it changes to get accurate results. Based on the report share by The White House, there is no generic model for SCADA forensics and one needs to be made that is able to run without interfering with the system (The White House, 2013). The need to provide students with skills and expertise to defend these critical assets is high, and state and government agencies support research and teaching initiatives in these fields (The White House, 2013; Department of Homeland Security, 2003; Control engineering salary and career survey, 2013).

NEED

The ICS critical infrastructure has gained much attention due to the effectiveness of attacks to cause physical harm to the ICS infrastructure. Due to major concerns, the study and research of ICS is very important in academia, especially in the fields of engineering and computer information. Therefore, educating students on how to mitigate potential cyber-attacks requires more advanced core curriculum and laboratory infrastructure. Educating the future workforce, who will be utilizing such systems as part of daily operations, requires interdisciplinary curricula and collaborations between the fields of comput-

Dr. Ulan Dakeev is serving as an Assistant Professor of Engineering Technology in the College of Science and Engineering Technology at Sam Houston State University. He served as an assistant professor at Texas A&M University – Kingsville, lecturer at University of Michigan – Flint, and a design engineer at John Deere Waterloo Dr. Dakeev holds a B.S. in Industrial Engineering from the International Black Sea University, an M.S. in Industrial Management, and Doctorate in Technology from the University of Northern Iowa. He is an active member of member of ATMAE, IAJC, ASEE, Epsilon Pi Tau National Engineering Honor Society. Dr Pecen is a certified NCCER instructor for 21 trade skills. His research areas include Virtual and Augmented Reality, Motivation and Engagement of Students and Employees.

er information science and engineering to teach both hardware and software vulnerabilities (Foreman, Turner, & Perusich, 2015; Foreman, et al., 2012; Cherdantseva, et al., 2016; Slay & Sitnikova, 2008). Due to cyber-security and digital forensics education being part of the computer information science curricula and ICS as part of engineering curricula, it becomes difficult to determine how to educate students in both fields of the study. There are two educational learning parts in ICS; hardware and software. The hardware is the physical infrastructure of ICS, including PLCs, input/output devices, network switches and routers etc. where software infrastructure encompasses network programming, server and database management, analysis of network for potential cyber-attacks, and script programming, etc. In order to further study ICS, the aforementioned challenges are addressed by developing a cyber-security mobile laboratory unit that serves both the computer information science and engineering fields.

It is typical to teach automation and control systems (including PLCs) in computing information science and engineering curricula. However, the security part of the automation and control system is missing from the curriculum, unless there is a cyber-security/digital forensics curriculum available. It is necessary to provide training and education for both control system engineering students and computer information science students who will become professionals in protecting such systems against cyber-attacks in the future. Although there are major initiatives from the state and federal agencies, there exists very limited educational resources related to the ICS and cyber-security based on the literature review of educational studies by Foo, Branagan, & Morris, 2013; Whitman & Mattord, 2004; Streff & Zhou, 2006; Francia, 2011; Ellis, 2008. It is critical to provide knowledge, skills, and security awareness in engineering and computing information science curricula to protect critical infrastructure against cyber-attacks (Foo, Branagan, & Morris, 2013; Whitman & Mattord, 2004; Streff & Zhou, 2006; Francia, 2011; Ellis, 2008).

PURPOSE

The purpose of this research study is to allow access from both disciplines (Computer Science & Cyber Security and Electronics & Computer Engineering Technology) and open an opportunity to study ICS and cyber-security vulnerabilities with simulated attacks to system components. The curriculum aims to bridge this gap by providing theoretical and practical exercises that will raise the awareness and preparedness of students. The SCADA/ICS system is designed to be accessible to students of either discipline, which allows this important subject to be included in either curriculum quickly and without the need for developing a new course. The modules explore the unique network protocols and security measures implemented in ICS from the perspective of maintaining reliable process control, including known vulnerabilities and attacks. The modules also explore methodologies for intrusion detection, forensics, and attack mitigation as uniquely applied to ICS. Finally, a lab-scale ICS platform is developed to serve as a cyber-security trainer for students from both disciplines, including sample lab experiments that encourage interdisciplinary cooperation towards achieving the common goal of a critical infrastructure cyber-security. In order to assess the impact of these modules on students, a survey was developed to measure the understanding of the unique aspects of ICS cyber-security both before and after module presentation and laboratory participation.

To further evaluate the security of such systems, several students from a research team began to develop a laboratory that would allow students and researchers to conduct assessments for vulnerabilities in the cyber-security of industrial control. In addition to security assessments, the lab may serve as a learning platform for various Engineering Technology related course work. The SCADA lab's intended functionality is to provide a realistic imitation of an industrial control SCADA system. The lab can be used to investigate multiple research areas for security purposes such as penetration assessment and testing, SCADA protocols analysis, vulnerability assessment and testing, and SCADA forensics research (O'Leary, 2006). This laboratory is intended to be used for both Digital and Cyber Forensic Engineering Technology and other Engineering Technology programs (e.g., Electronics Technology, and Electronics and Computer Engineering Technology). The laboratory may serve for undergraduate computer science and engineering technology courses as well as research projects in the areas of instrumentation and interfacing, automation and control systems, robotics technology, microcontroller applications, control technology, PLCs, process control, digital forensics, and cyber-security.

Laboratory Design and Development

Using the information above, a lab's SCADA architecture was carefully designed. For the intended use case of the lab, it was important to incorporate a wide range of hardware and software into the SCADA system so that the testing environment could be as diverse as possible. PLCs from different manufacturers including Allen Bradly, Automation Direct, Schneider, and Eaton were implemented into the system with various transducers and outputs. Following is a list of the PLCs and their associated inputs and outputs included in the lab is listed in Table 1.

Table 1: PLC Units and Associated Input & Output Components

Part#	PLC	Interfaced Devices
1	Eaton XC-CPU202	• Buzzer • LED Lights
2	Direct Logic 06 Koyo	• Tower Light • Buzzer • Rotary Encoder
3	Automation Direct Productivity 3000	• Humidity Sensor • Picking Sensor and LED Light
4	Allen Bradley MicroLogix 1100	• Photoelectric Proximity Sensor • LED Light
5	Schneider M221	• Air Velocity Sensor • LED Light

Additional hardware was also installed. A protocol converter was included to ensure compatibility between devices and to provide the ability to enable additional SCADA protocols throughout the system. Three of the three HMIs installed include dedicated hardware from Allen Bradley and Weintek. A microcontroller with 802.11 wireless capabilities and a wireless IP camera were also installed. Following is a list of the remaining hardware included in the lab Table 2.

Table 2: A List of SCADA/ICS Hardware

Part #	SCADA/ICS Hardware
1	Red Lion DSPLE Protocol Converter
2	Weintek EMT3120A
3	Allen Bradley Panel View 600
4	IP Camera
5	ESP8266 Wireless Microcontroller with smoke sensor
6	Firewall and a 24-port network switch
7	Wireless Access Point
8	5xDesktop Computers

The training materials used for the project were chosen for their cost-effective price, availability, and portability. After thorough research, Schneider Electric was chosen as the optimal company to supply the equipment, parts, and software. An OPC server was used as a middle component between the protocols of the PLC components and the SCADA client system. The only "free" OPC server found was Matrikon and Kepware, which had evaluation versions with two-hour limits. A training environment was developed to expose students to the various sensors and industry-standard protocols (e.g.) MODBUS. The learning objectives were to become proficient where students expected to be able to do the functions of a SCADA system (I.E., control & acquire data) in the roles of a SCADA system; how to wire up a PLC to the system and various sensors; program the PLCs; identify, configure, and test communications; and troubleshoot and create HMIs for operating the equipment. After the course, most students felt well versed in what a SCADA system is and how it works.

The core infrastructure of the SCADA lab is shown in Figure 1.

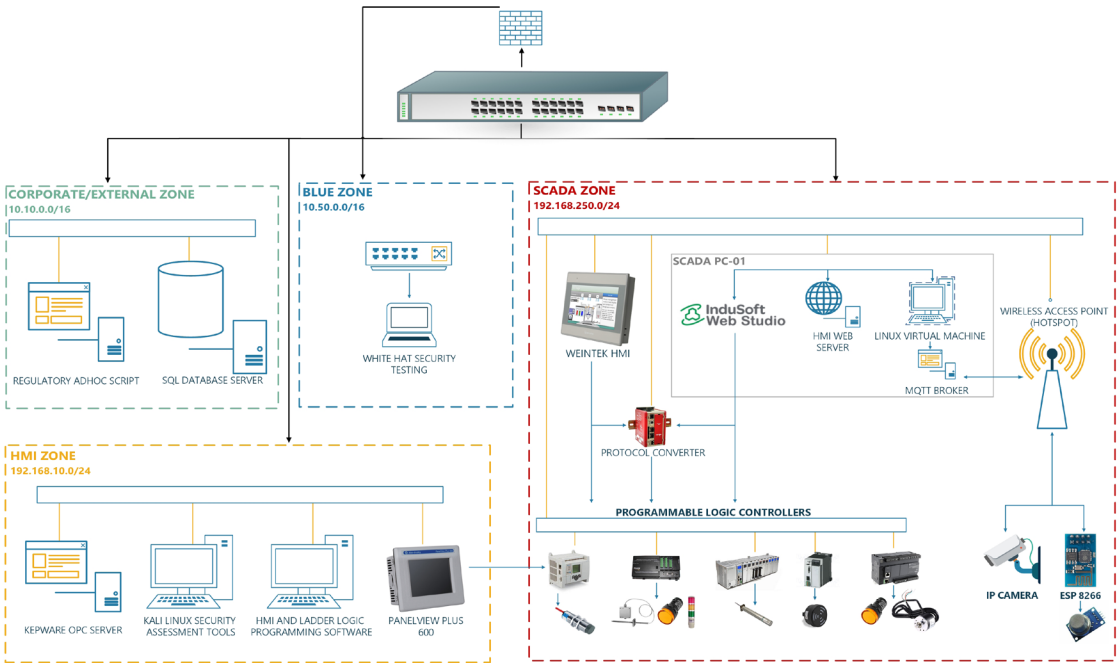

Figure 1: Laboratory Network Design of the Proposed SCADA Scheme

As shown in Figure 1, the network switch consists of three subnets: SCADA, HMI, Corporate/External. Additionally, a fourth subnet exists directly through the firewall, which will be discussed later. The design layout is intended to imitate multiple SCADA architectures, where data acquisition and control is performed either locally or remotely. The InduSoft and Weintek HMIs can interface with PLCs using three different methods: directly through the PLC's native communication protocol, through the Red Lion Protocol Converter, or through the OPC server. Implementations of the three possible communication methods are included in the InduSoft and Weintek HMI. The SQL database server (historian) is hosted on the corporate/external zone and communicates directly with InduSoft. A regulatory script is implemented to read data from the historian every hour and save the data in the form of .csv files. If desired, the .csv files can then be loaded into a spreadsheet for further interpretation.

InduSoft™ HMI Screen

The InduSoft HMI screen was developed as a combination of programming with tags and VBScript as shown in Figure 2 (2a, 2b, 2c). The screen was designed to interface with all PLCs in the lab using one or more of the communication methods provided by the lab's architecture. Status indicators, continuous and point level measurement readings, and manual control inputs are displayed throughout the screen. Utilizing the features provided by InduSoft, the state of the screen is synchronized with an HTML file in

a directory that is hosted on a local HTTP server. This enables remote access and control of the InduSoft HMI through any web browser on the network.

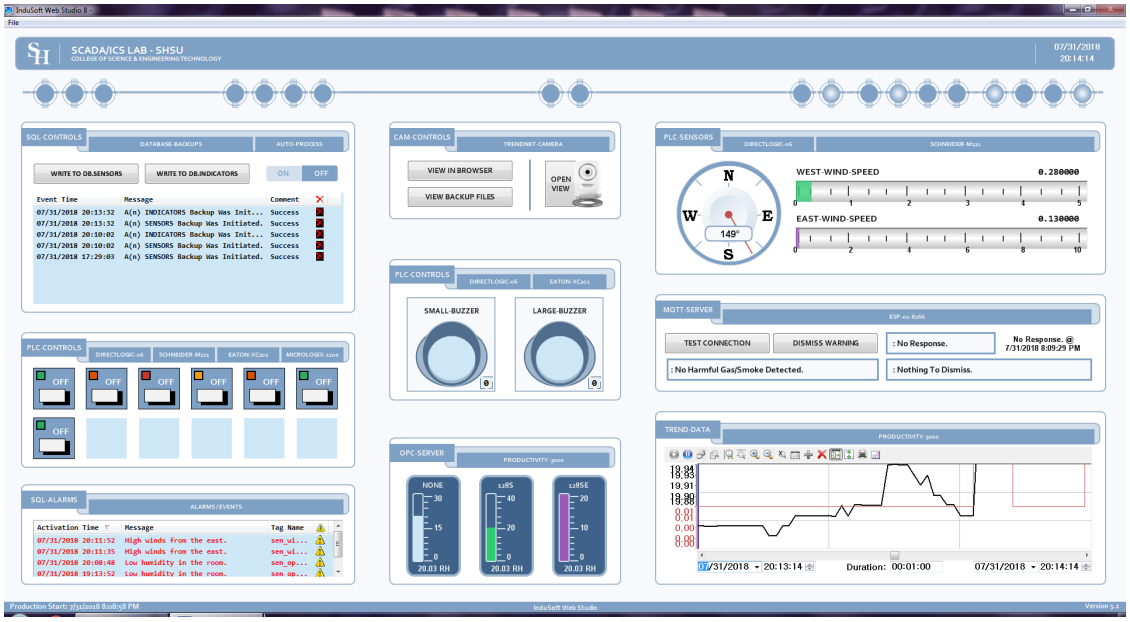

Figure 2a: InduSoft HMI Screen

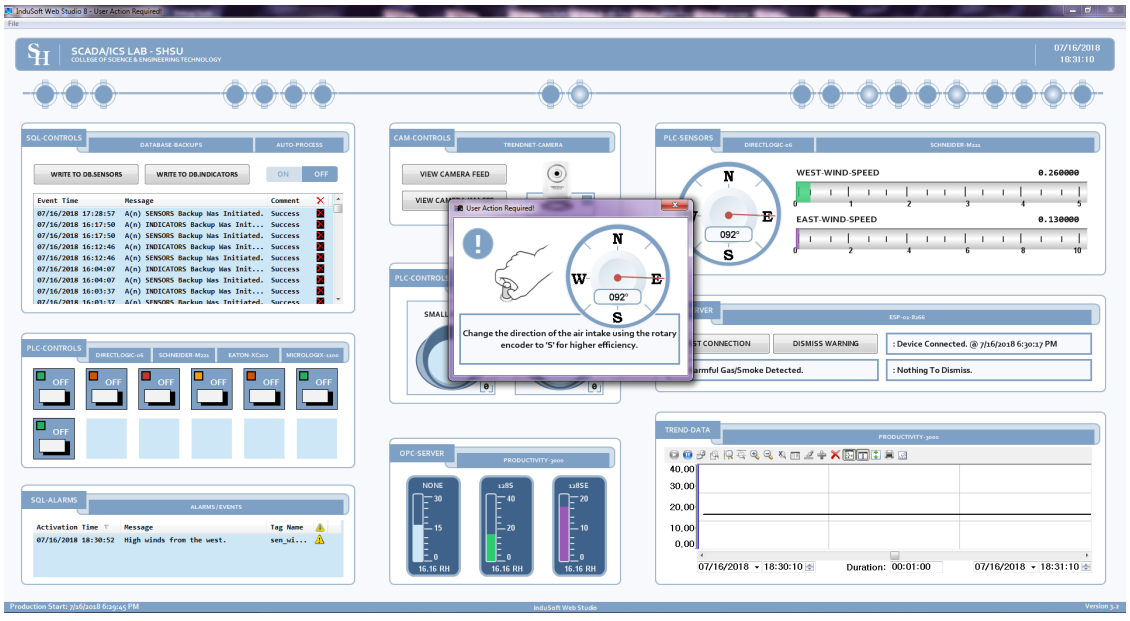

Figure 2b: Popup for Adjusting Simulated Air Intake Valve

Figure 2c: Weintek HMI Screens

An automatic process control simulation was also incorporated into the screen. The automatic process control simulation is designed to cycle through the available outputs across all PLCs at consistent and evenly distributed timings. The significance of providing even and repetitive timings is discussed in more detail in the security section of the paper. At the end of the automatic process, all input data is sent to the historian and the cycle repeats. The automatic simulation operates asynchronously, allowing manual inputs to function while the process is running. Each cycle of the automatic process is intended to generate network traffic for all available SCADA protocols. Figure 3 shows the photo of the research laboratory environments. The initial setups took place in the room where all the components were installed permanently.

Figure 3: Established SCADA Research Lab Environment

Transitioning to Mobile Lab Concept

There was a necessity to move the hardware between the labs and classrooms for experimental project purposes. The project team came up with a new design and moved all the hardware to a portable unit. The mobile unit has all the hardware installed and tested and has the potential to move between laboratories and buildings. This new idea also allows the project team to install more components to the back of the unit. A very important benefit of the portability of the new set up is the interchangeability it allows between the CS department's digital forensics program and the ECET program. Figure 4 (4a and 4b) shows a new mobile unit.

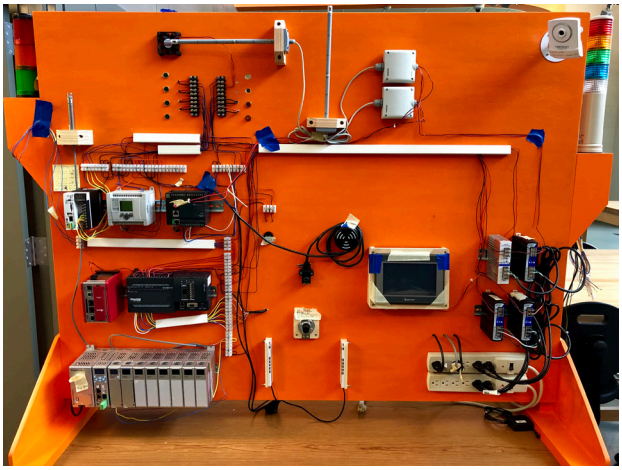

Figure 4a: Mobile SCADA Lab – Closer View

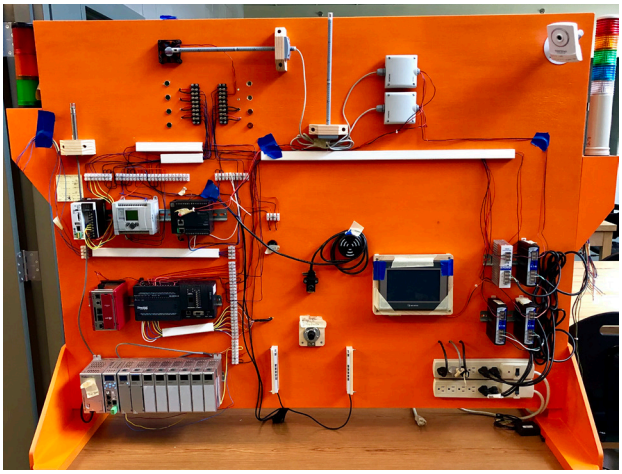

Figure 4b: Mobile SCADA Lab – Remote View Showing the Portable Table

Preliminary Tests and Studies

Early cases of student involvement regarding SCADA security have yielded several notable observations. Among the first assessments conducted by student participants include network stress tests in the form of protocol analysis via packet captures and the denial of service attacks. For both test cases, the automatic process control simulation of the InduSoft runtime was used. Denial of service attacks were performed against the InduSoft runtime, protocol converter, OPC server, and all PLC's. Each device was tested against UDP flood and SYN flood (TCP) attacks. Additionally, packet captures were made for each test in the form of .pcap files so that the results could be further evaluated. The results indicated that all PLC's in the lab as well as the Red Lion protocol converter were vulnerable to UDP floods. During the experiment, any targeted hardware device could be taken offline in a fraction of a second through a UDP flood attack, even if the targeted device did not utilize UDP for any sort of communication. When performing such attacks, the InduSoft HMI was capable of indicating that each targeted device was taken offline for all components excluding the DirectLogic Koyo PLC. Interestingly enough, when the Koyo PLC was taken offline via UDP flood, the InduSoft HMI would continue to report the enabling and disabling of outputs on the PLC and the falsely reported events would be documented in the SQL database.

The lab proved to be more resilient against SYN flood attacks. All PLC's appeared to ignore the SYN requests from the performed SYN floods. Numerous TCP ports were targeted during these trials. This assessment suggested that the component of the InduSoft runtime that operates as the master terminal

unit of the SCADA system is most vulnerable to SYN flood attacks. During this attack, no systems were brought offline, but significant latencies were introduced. When the InduSoft network port associated with supervisory control was targeted by a SYN flood attack, the timings of the automatic process control simulation were no longer consistent. All functions of the process were delayed or expedited by a range of ~.1-2 seconds. This inconsistency is apparent in the timestamps of the events recorded in the data historian. Such inconsistencies introduced by the attack are also likely to be apparent in the packet capture for the trial.

Protocol analysis assessments were conducted using Wireshark. In the lab's current configuration, the following communication protocols are utilized: Modbus/TCP, Common Industrial Protocol (CIP), CODESYS ARTI, OPC, Message Queuing Telemetry Transport (MQTT), ECOM/ UDP. Efforts were made by students to identify and analyze the packets of each protocol mentioned above. During the assessment, live sensor data was easily identifiable within the data frames of the unencrypted protocols. Additionally, comparisons were made using the three variants of OPC implemented in the lab: unencrypted, signed, signed and encrypted. To further the study, a more in-depth protocol analysis was performed on the observed Modbus network traffic. Using Wireshark to monitor the active Modbus traffic from the Schneider M221, Productivity 3000, and protocol converter, it was observed that the protocol identifier was always 0x0000. Since Modbus is predominately an openly published and royalty-free protocol (Modbus application protocol, n.d.), public functions codes were successfully identified from all Modbus traffic originating from the protocol converter. However, it was discovered that the Productivity 3000 exclusively used user-defined functions to perform commands that are supported by public function codes, such as reading input registers. Furthermore, an unexpected undocumented and reserved function code was also observed on the Schneider M221 PLC.

Implementation of an HTML Web Viewer

A common feature for SCADA systems includes the ability to remotely view and control an HMI screen. An important component added to the SCADA lab includes the ability to perform vulnerability assessments and testing on HTML based remote HMI screens. For this feature to be possible, a Hypertext Transfer Protocol (HTTP) server is required to host parts of the SCADA system's core file directory which may contain sensitive information that is valuable to an attacker. Additionally, if an attacker manages to circumvent the authorization for remote HMI access, then the attacker would have full remote control of the HMI screen. To enable vulnerability assessments and evaluations on remote HMI web viewers, the lab environment was set up to allow all subnets in the network to access the HMI web viewer and its authentication is limited to weak username and password credentials.

Implementation of HMI Screens

The main SCADA system software in the lab is conducted through InduSoft web studio. While SCADA protocols are standardized across most major industrial control and automation software suits, it is important to implement alternative SCADA software solutions into the lab so that assessments and comparisons can be made between platforms. For a secondary HMI, an Allen Bradley PanelView Plus 600 was introduced to the lab. The PanelView is a particularly appealing component for vulnerability assessment and security analysis because it relies on dedicated hardware running on the Windows Embedded Compact 6.0 operating system. It may be possible that the unconventional operating system could expose a SCADA system to undocumented vulnerabilities and exploits. The PanelView HMI is configured with the FactoryTalk View Studio software and has SCADA features configured for data acquisition and control of an Allen Bradley Micrologix 1000 PLC through an RS-232 serial connection. The communications configuration for this HMI application is unique because it allows for assessments of a SCADA system where the PLC is wired through a serial connection opposed to Ethernet.

Network Configuration

Since the lab was intended to simulate the mediocre security practices that are commonly found throughout the industry, the SCADA lab has a rather minimalistic network configuration. Most security features within the firewall are disabled and passwords are short and simple. The network is split into three subnets labeled SCADA, HMI, and EXTERNAL. Isolating the network into three different subnets allows the lab to simulate three separate remote networks that collectively provide data and functionalities to the human machine interface of the lab. The computers on the external subnet are installed with

objectively insecure SQL servers that communicate with the indusoft SCADA. The information in this network traffic is intended to provide revealing information if someone were to eavesdrop.

Indusoft HMI SCADA Software

The HMI/SCADA software is packaged into the software labeled indusoft web studio. The HMI is configured to simulate a chemical batching process that is intended to utilize the following protocols -MODBUS, TCP/IP, OPC-DA, OPC-UA, ARTI CODESYS, DNP3, KOYO, and IEC 60870-5-104. These are the protocols that are most commonly used in real SCADA systems. Since the Eaton and DirectLogic06 PLCs are only capable of utilizing a few of these protocols, the rest are implemented through simulators. The network traffic generated from these protocols are intended to be useful for security and forensic analysis.

Vulnerability Analysis and System Audit

After the hardware and software implementations and configurations, the system and its modules are tested against cyber-attacks. The goal of the performed simulated attacks is to teach students how to identify the weaknesses of SCADA system and its components and analyze the system's responses by collecting the evidential data. In order to perform simulated attacks, a couple of forensic tools are installed in the attacker system. One of the four computer stations had Linux Kali operating system installed for the purpose of simulated attacks. The Kali/Linux operating system is used to run a series of penetration testing tools such as Nmap (Nmap - penetration testing tools, 2018), Zmap, Miranda (Miranda - penetration testing tools, 2018), jSQL Injection (jSQL tool - penetration testing tools, 2018). Additionally, Low Orbit Ion Cannon (LOIC) (Abatishchev, 2018) tool is installed on one of the Windows desktops and used to perform IP (Internet Protocol) flooding attacks. Low Orbit Ion Cannon is a tool that performs denial of service attack (DoS) in the form of UDP (User Datagram Protocol) flood attack. Moreover, Wireshark (Gerald C. et al., 2008) network packet analysis is also installed and utilized to detect and filter the network traffic in SCADA and the database protocols. For the simulated attacks scenarios the four-step approach proposed by Chris et al. (Johnson, Harkness, & Evangelopoulou, 2016; Taveras, 2013) is adapted to current experiments.

- Stage one- Identify vulnerabilities
- Stage two- Identify attack methods
- Stage three- Implement immediate risk reduction
- Stage four- Implement long-term solutions

Forensics analysis of SCADA system constitutes a different process than conventional forensic procedures. In SCADA forensics the analysis of data, presentation of data, and acquisition of data is performed (Rafique & Khan, 2013). There are mainly two types of data acquisition methods namely static and live acquisition. The former is the traditional approach in which the system needs to be shut down before the acquisition. In the latter data is gathered and analyzed while the system is running. Volatile and non-volatile data can be acquired during the live acquisition. The forensic investigator simply cannot turn off the SCADA system for data acquisition (Naedele, 2007) because of the availability of volatile data. If the system is turned off it is possible that the volatile data will be destroyed. Hence, live forensic (Adelstein, 2006) is a viable solution particularly for forensic analysis of SCADA system.

Penetration Testing

In this section, the performed attacks and their consequences are presented. A series of attacks are utilized in order to test strengths and weaknesses of the SCADA laboratory during the course of experiments. Table 3 and 4 show these attacks on the corresponding hardware and the result of the attacks.

During the simulation experiments, the only test case that was maliciously affecting the SCADA system's operation was a type of Denial of Service Attack called IP flooding using UDP. In order to perform the IP flooding attack, Low Orbit Ion Cannon tool is used against the SCADA system's sensors. Particularly, the attacks are successfully performed on Humidity Sensor, Wind Sensor, Rotary Encoder, Proximity Sensor, KOYO Led Lights, and the Buzzer. All the sensor values along with associated timestamps are given in Table 5 for both regular working and attacked conditions.

Table 3: Hardware Environments used During the Attack Experiments

PLC Model	Attached Hardware
Eaton XC-CPU202	Buzzer, LED Lights
DirectLogic 06	Tower Light, Buzzer, Rotary
Koyo	Encoder Humidity Sensor, Picking
Automation Direct	Sensor, LED Light Photoelectric
Productivity 3000	Proximity Sensor, LED Light
Allen Bradly	Air Velocity Sensor, LED Light
MicroLogix 1100	
Schneider M221	

Table 4: Unsuccessful Attack Cases and their Corresponding Results

Case #	Test Cases	Software Tool Used	Test Result
1	Test for MODBUS protocol traffic	Wireshark	Pass
2	Test for OPC DA protocol traffic	Simulator logs	Pass
3	Test for OPC UA protocol traffic	Wireshark	Pass
4	Test for KOYO protocol traffic (KOYO is transmitted as UDP packets)	Wireshark	Pass
5	Test for EATON's Code SYS ARTI protocol traffic	Simulator logs	Pass
6	Test for DNP 3.0 protocol traffic	Wireshark	Pass
7	Verify network for IE104 (IEC 60870-5-104) protocol traffic	Simulator logs	Pass
8	Verify if Direct 06 PLC is configured to respond via HMI (Indusoft) interface	HMI alarms and logs	Pass
9	Verify if Eaton PLC is configured to respond via HMI (Indusoft) interface	HMI alarms and logs	Pass
10	Test for password strength using password cracker tools	John the Ripper	Pass
11	Perform a penetration test using any known exploit against the lab network	Metasploit	Pass
12	Test for Windows security patches to expose backdoors	Microsoft Baseline Security Analyzer	Pass
13	Test for open and vulnerable ports against lab network	Nmap	Pass
14	Test for SQL Injection against lab network	jSQL Map	Pass

Table 5: Attack Results Analysis on Database

	Timestamp	KOYO_Humidity	MODBUS_Wind	KOYO_encoder
Regular	11:53:58	23.023	0.01	180
Attacked	11:55:47	**6.513**	0.01	204
Regular	11:55:22	6.29	0.16	204
Attacked	11:55:34	6.29	**0.01**	204
Regular	11:56:23	6.257	0.01	204
Attacked	11:56:47	6.15	0.18	**178**

Forensic Analysis and Incident Response

Experiments showed that, the SCADA lab is not vulnerable against a significant number of performed attacks. After the attacks, the SCADA system was forensically analyzed. In order to carry out a forensically sound investigation, a 7-step forensic investigation model stated by Tina et al. in (Wu, Disso, Jones & Campos, 2013) is used.

- Phase 1- Identification and Preparation
- Phase 2- Identifying data sources
- Phase 3- Preservation, Prioritizing, and Collection
- Phase 4- Examination
- Phase 5- Analysis
- Phase 6- Reporting and Presentation
- Phase 7 Reviewing Results

The summary of the effects to SCADA system input/ output devices are listed below:

KOYO LED lights: LED lights (Green, Yellow, Red) are connected to the InduSoft and can be controlled manually via the HMI screen. According to the proper operations of the KOYO LED Lights, when the "ON" button is pressed for any color, its appropriate light turns on. Before the attack is performed on KOYO Led lights, the lights' IP addresses are recorded on the LOIC tool as '19.168.240.2'. While the attack is performed on the system, the LOIC tool prevented any associated lights being turned on. This was also observed on the HMI screen.

Humidity Sensor: This humidity sensor is connected to the Automation Direct Productivity 3000 PLC unit, and it communicates directly with InduSoft. Any instant changes in humidity can be observed on the HMI screen. Before performing the IP flooding attack on the Humidity Sensor, the sensor and its data transfer to the database is tested. Every 12 seconds cycle, the InduSoft was able to write the data to the database. The UDP flooding attack started with LOIC tool on the sensor's IP address '19.168.250.10'. As shown in Table 3, at 11:53:58 the system is started and the humidity level is increased. After the increase can be seen through the HMI screen, the current data at that time is collected. The humidity level was 23.023 on the database, and while increasing the humidity, to perform the attack to analyze the sensor's operation is started. The attack stopped the sensor's operation at 11:55:47 and the humidity level decreased immediately. The changes on the data can be analyzed both the HMI screen and the database.

Wind Sensor: Similarly, this sensor relates to the PLC and communicates directly with InduSoft. The wind changes can be observed and analyzed via the HMI screen. Users can increase the wind level by blowing out to the sensor. Before performing the flood attack on the wind sensor, the sensor and its data transfer to the database is tested. The UDP attack started using LOIC tool on the sensor's IP address '19.168.250.3'. As shown in Table 3, the system is started and the wind level is increased at 11:55:22. As soon as the increase is observed on the HMI screen, the data in the database is collected. Regularly, the Lab's wind level is 0.01, and after increasing the wind level manually, the wind level became 0.16 in the database. While the humidity is increased, the same attack is launched to analyze the changes in the sensor's operation. The attack stopped the sensor's operation at 11:55:34 and the wind level decreased to 0.01 immediately.

Rotary Encoder: This encoding sensor is connected to Direct Logic 06 KOYO PLC and communicates directly with InduSoft. The Rotary changes can be observed on the HMI screen. Users can change the degrees by rotating the sensor and the rotation. The rotation can be maximized at 360-degree and minimized at 1-degree. Before performing the flooding attack on the rotary encoder sensor, the sensor and its data transferred to the database is tested. The successful data transfer was observed in the database. The UDP attack started with LOIC tool on the sensor's IP address '19.168.250.2'. As shown in Table 3, at 11:56:23 we have started the system and rotated the rotary encoder to change the degrees. During the observation of the changes in degree through the HMI screen, the related data from the database is also collected. The rotation degree was 204 before we launched the attack. After the attack, the sensor's operation has stopped at 11:56:47 and the rotation changes in the degree stopped at 178. Even though the rotation made manually while the attack was performed, the rotary degree changes stopped at both the HMI screen and the database.

Buzzer: This sensor is connected to EATON XC-CPU202 PLC and communicates directly with InduSoft. The changes on the Buzzer can be observed on the HMI screen. Users can activate Buzzer manually by pressing the Buzzer button on the HMI screen. The UDP attack started with LOIC tool on the Buzzer's IP address '19.168.250.3'. After launching the attack, the buzzer's operation stopped. It took a few minutes to reactivate Buzzer's operation after the UDP attack.

Student Involvement and Education Activities

Project-Based Learning (PBL) and Problem Based Learning curricula are becoming the norm for many engineering and science fields, business, and medicine to help prepare students for the real-world (Dym, Agogino, Frey, & Leifer, 2005), (Macias-Guarasa, Montero, San-Segundo, & Nieto-Taladriz, 2006). PBL pedagogy centers learning on the activity of the student. An approach to preparing students to become industrial designers is to include design projects throughout the curriculum, hence PBL curriculum. The accreditation agency, ABET, among other entities, influenced engineering programs into including a major capstone around 1995 to 1997 (Dutson, Todd, Magleby, & Sorensen, 1997). For computer engineering curriculum, the lab only courses (Areibi, 2001), (Newman, Hamblen, Member, Hall, & Member, 2002) slowly evolved to include both labs and final projects. The senior capstone has been studied to help understand how to prepare students for this culminating experience (Lesko, 2009), (Goldberg, 2009). This project started with the announcement of Enhancing Undergraduate Research Experiences & Creative Activities (EURECA)'s Faculty and Student Team (FAST) project/grant announcements where undergraduate students work under one or more faculty supervisors for a summer project. This internal project provides summer stipend for the students and faculty and is very competitive due to many applications received by the committee to renew. Two students volunteered to be part of the project and filled out the application. The project was not among those applications were approved for the summer studies. However, office research and sponsored programs (ORSP) funded two students to work on the project. Both students were electronics and computer engineering technology (ECET) majors and then one computer science (CS) major student joined to team to help on the cyber-security part of the project. The project was supervised by an ECET and CS faculty who are experts in digital forensics and industrial automation & control fields. In Fall 2018, two of the students were already graduated and three new students were identified to take over the project for the future expansion of the project. During the experimental research, a mobile SCADA laboratory was developed, deployed, tested, and analyzed. The current state of the lab is fully functional and yet to be improved with new equipment. This lab is an indispensable resource for both undergraduate and graduate students for both research and coursework.

CONCLUSION

Industrial automation knowledge and skills in different levels are required in many engineering technology related positions and yet the workforce with this knowledge are hard to recruit. High schools and colleges need to provide industrial automation classes to transition students into their future jobs. Many surveys taken prove that there is a high need for industrial automation knowledge, and further surveys indicate that companies are having a hard time finding people skilled in technologies like PLC programming, automation, wireless technology, troubleshooting, etc.

If the new employees need to be trained, it's often difficult to get the employees proficient in all the combination of skills they need. Technicians need to understand the how and why of systems operations and problems instead of just guessing different possible solutions and seeing if they will work (Hsieh, 2016).

This project was initially launched to promote a center for digital forensics studies. The center has been inactive for a long time due to lack of interest from the faculty and the students until two of the faculty decided to involve students and stimulate the center with research projects. Since last year, seven students worked in the center having major duties to promote and activate the center. At present, the center/lab can be used for teaching and research purposes and attract more students who would like to study industrial control, SCADA security systems, digital forensics etc. Student feedbacks are very positive in terms of learning and involving hands-on projects. One major common feedback is an improvement on reporting and writing capabilities of the students who involved in the report and manual preparation phases of the project. The development content and lab resources are being part of instrument and interfacing and automation and control systems courses, but the resources will be used in

more course work needs for both engineering technology and computer science departments. More students are being interested and demonstrate desire to work in the SCADA lab/center and proposing new research ideas. This year, two of the students applied to EURECA's FAST project to get summer funds in order to work in the center.

References

Abatishchev. (2018). *Low orbit ion cannon-- penetration testing tools.*

Adelstein, F. (2006). Live forensics: Diagnosing your system without killing it first. Communications of the ACM. 49(2), 63-66.

Ahmed, I., Obermeier, S., Naedele, M., & Richard, G. (2012). SCADA Systems: Challenges for Forensic Investigators. 45, pp. 44-51. Retrieved from http://ieeexplore.ieee.org/xpl/articleDetails.jsp?reload=true&arnumber=6298895

Akelian, C. J. (2015). Incorporating SCADA modules into Introductory Programmable Logic Controller Curriculum. *In proceedings of the 122nd ASEE Annual Conference & Exposition.* Seattle, WA: American Society for Engineering Education.

Areibi, S. (2001). A first course in digital design using vhdl and programmable logic. *Paper presented at 31st Annual Frontiers in Education Conference. 1,* pp. 19-23. TIC. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.16.3048

Cardanes, A.A., Amin, S., Lin, Zong-Syun, Huang, Yulun, Huang, Chi-Yen, Sastry, S. (2011). Attacks against Process Control Systems: Risk Assessment, Detection, and Response. Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security March 2011 Pages 355–366 https://doi.org/10.1145/1966913.1966959

Cherdantseva, Y., Burnap, P., Blyth, A., Eden, P., Jones, K., Soulsby, H., & Stoddart, K. (2016). A review of cyber security risk assessment methods for SCADA systems. *Computers & Security,* 56, 1-27.

Control engineering slaray and career survey. (2013). Retrieved from https://www.controleng.com/single-article/control-engineering-salary-and-career-survey-2013/cd2a03c44fa44e6f1d-273c30dd7fa94c.html

Department of Homeland Security. (2003, Dec). *Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection.* Retrieved from Official website of the Department of Homeland Security: https://www.dhs.gov/homeland-security-presidential-directive-7

Dutson, Alan & Todd, Robert & Magleby, Spencer & Sorensen, Carl. (1997). A Review of Literature on Teaching Engineering Design. Journal of Engineering Education. 86.

Dym, C. L., Agogino, A. M., Frey, D. D., & Leifer, L. J. (2005). Engineering design thinking, teaching, and learning. *Journal of Engineering Education, 94,* 103-120. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.72.1593

Ellis, R. (2008). Critical infrastructure and control systems security: An interdisciplinary approach. *In proceedings of the 2008 IEEE Conference on Technologies for Homeland Security* (pp. 459-462). IEEE.

Ettercap. (n.d.). Retrieved from Ettercap Project: https://ettercap.github.io/ettercap/index.html

Foo, E., Branagan, M., & Morris, T. (2013). A proposed australian industrial control system security curriculum conference paper. *In proceedings of the 2013 46th Hawaii International Conference on System Sciences.* doi:10.1109/HICSS.2013.55

Foreman, C., Hieb, J., Graham, J., & Ragade, R. (2012). A curriculum model for industrial control systems cyber-security with sample modules. *In proceedings of the IS-CA 27th International Conference On Computers and Their Applications,* (pp. 179-183). Las Vegas, NV.

Foreman, C., Turner, M., & Perusich, K. (2015). Educational modules in industrial control systems for critical infrastructure cyber security. *In proceedings of the 2015 ASEE Annual Conference & Exposition,* (p. 23911). Seattle, Washington.

Francia, G. A. (2011). Critical Infrastructure Security Curriculum Modules. *In proceedings of the Information Security Curriculum Development Conference,* (pp. 54-58). New York, NY.

Gerald, C. e. (2008). Wireshark-network protocol analyzer. Version 0.99. Retrieved from www.wireshark.org

Gerald, C. (n.d.). *Wireshark Project.* Retrieved from Wireshark: www.wireshark.org

Goldberg, J. (2009). Preparing students for capstone design [senior design]. *Engineering in Medicine and Biology Magazine, 28*(6), 98-100. Retrieved from https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=5335729

Goldman, D. (2013, Jan). Hacker hits on U.S. power and nuclear targets spiked in 2012. *CNN Money.*

Hsieh, S. (2016). Skill Sets Needed for Industrial Automation Carrers. *In proceedings of the ASEE's 123rd Annual conference & Exposition.* New Orleans, LA: American Society for Engineering Education.

Johnson, C. W., Harkness, R., & Evangelopoulou, M. (2016). *Forensic attacks analysis and the cyber security of safety-critical industrial control systems. In proceedings of the 34th International System Safety Conference.* Orlando, FL.

JSQL tool - penetration testing tools. (2018). Retrieved from KALI TOOLS: Tools.kali.org

Lesko, C. J. (2009). Building a framework for the senior capstone experience in an information computer technology program. *In proceedings of the 10th ACM conference on SIG-information technology education,* (pp. 245-251). Retrieved from http://doi.acm.org/10.1145/1631728.1631804

Luiifj, E. (2012). Understanding cyber threats and vulnerabilites. (J. Lopez, Ed.) *Critical Information Infrastructure Protection,* 52-67.

Macias-Guarasa, J., Montero, J., San-Segundo, R. A., & Nieto-Taladriz, O. (2006). A project-based learning approach to design electronic systems curricula. *IEEE Transactions on Education, 49*(3), 389-397. Retrieved from http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1668283

Meier, J. D., Mackman, A., Dunner, M., Vasireddy, S., Escamilla, R., & Murukan, A. (n.d.). *How to: Use the Microsoft baseline security analyzer.* Retrieved from Microsoft: https://msdn.microsoft.com/en-us/library/ff647642.aspx

Miranda - penetration testing tools. (2018). Retrieved from KALI TOOLS: Tools.kali.org

Modbus application protocol. (n.d.). Retrieved from http://www.modbus.org/docs/Modbus_Application_Protocol_V1_1b3.pdf

Morris, T., Srivastava, A., Reaves, B., Gao, W., Pavurapu, K., & Reddi, R. (2011). A control system testbed to validate critical infrastructure protection concepts.

Naedele, M. (2007). Addressing it security for critical control systems. *In proceedings of the IEEE 40th Annual Hawaii International Conference on In System Sciences* (p. 115).

Newman, K. E., Hamblen, J. O., Member, S., Hall, T. S., & Member, S. (2002). An introductory digital design course using a low cost autonomous robot. *IEEE Transactions on Education, 45,* 289-296.

Nguyen, V., Tran, Q., & Besanger, Y. (2016). SCADA as a service approach for interoperability of micro-grid platforms. *Sustainable Energy, Grids and Networks, 8,* 26-36. Retrieved from https://www.sciencedirect.com/science/article/pii/S235246771630056X?via%3Dihub

Nmap - penetration testing tools. (2018). Retrieved from KALI TOOLS: https://tools.kali.org/

O'Leary, M. (2006). A laboratory based capstone course in computer security for undergraduates. *In proceedings of the 37th SI GCSE technical symposium on Computer science education* (pp. 2-6). New York, NY: ACM.

OWASP Zed Attack Proxy Project. (n.d.). Retrieved from OWASP: www.owasp.org/index.php/ZAP

Rafique, M., & Khan, M. (2013). Exploring static and live digital forensics: Methods, practices and tools. *International Journal of Scientific & Engineering Research, 4*(10), 1048-1056.

Rouse, M. (2005, Sep). SCADA (supervisory control and data acquisition). Retrieved from https://whatis.techtarget.com/definition/SCADA-supervisory-control-and-data-acquisition

Sanger, D., & Schmitt, E. (2012, July 27). Rise Is Seen in Cyberattacks Targeting U.S. Infrastructure. *The New York Times New York Edition,* p. A8. Retrieved from http://money.cnn.com/2013/01/09/technology/security/infrastructure-cyberattacks/index.html

Scheffer, E., Wibberley, D., & Beets, N. (2002). What the future holds for SCADA systems and process automation. 19(7), 40-42.

Slay, J., & Sitnikova, E. (2008). Developing SCADA systems security course withing a systems engineering program. *In proceedings of the 12th Colloquium for Information Systems Security Education.* University of Texas, Dallas, TX: University of South Australia.

Stirland, J., Jones, K., Janicke, H., & Wu, T. (2014). Developing cyber forensics for SCADA industrial control systems. *In proceedings of the International Conference on Information Security and Cyber Forensics.* Kuala Terengganu, Malaysia: SDIWC.

Stouffer, K., Falco, J., & Kent, K. (2007). *Guide to supervisory control and data acquisition (SCADA) and industrial control systems security.* Special Publication. Retrieved from https://www.researchgate.net/publication/246350235_Guide_to_Supervisory_Control_and_Data_Acquisition_SCADA_and_Industrial_Control_Systems_Security

Streff, K., & Zhou, Z. (2006). Developing and enhancing a computer and network security curriculum. 4-18.

Taveras, N. P. (2013). SCADA live forensics: Real time data acquisition process to detect, prevent or evaluate critical situations. *In proceedings of the 1st Internation Symposium for ICS & SCADA Cyber Security Research (pp. 24-26). Azores, Portugal:AIIC.*

The White House. (2013). *Executive Order -- Improving Critical Infrastructure Cybersecurity.* Retrieved from The White House: https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity

Valli, C. (2009). SCADA forensics with snort ids. *In proceeding of WORLDCOMP2009, Security and Management 2009* (pp. 618-621). Las Vegas, NV: CSREA Press.

Velankar, A., & Mehta, A. (2002). Latest trends in SCADA for process automation. *In proceedings of the National Conference on Industrial Automation and Intelligent Systems,* (pp. 9-11).

What is OPC? (n.d.). Retrieved from OPC Foundation: https://opcfoundation.org/about/what-is-opc/

Whitman, M. E., & Mattord, H. J. (2004). Designing and teaching information security curriculum. *In proceedings of the 1st annual conference on Information security curriculum development* (pp. 1-7). Ney York, NY: ACM.

Wu, T., Disso, J. F., Jones, K., & Campos, A. (2013). Towards a SCADA forensics architecture. *In proceedings of the 1st International Symposium for ICS & SCADA Cyber Security Research, 12.*