SCADA Testbed for Vulnerability Assessments, Penetration Testing and Incident Forensics

Sundar Krishnan
Department of Computer Science
Sam Houston State University
Huntsville, TX
Email: skrishnan@shsu.edu

Mingkui Wei
Department of Computer Science
Sam Houston State University
Huntsville, TX
Email: mwei@shsu.edu

Abstract—**Industrial control systems are critical assets as they interact with real-life 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 for cyber-attacks. The need for skilled expertise starting at the academic level in defending and investigating these critical assets is ever growing. In this paper, the authors design and deploy a Supervisory Control and Data Acquisition (SCADA) lab at Sam Houston State University (SHSU) with a limited budget. The lab is designed to stimulate a near-world industrial setting specifically for Industrial cyber-security research (penetration testing, vulnerability analysis and incident forensics) as an accompaniment to the digital forensics education curriculum at the University.**

I. Introduction

Computer systems have outgrown in the last decades such that they connect all aspects of an enterprise IT ecosystem. Industrial control systems have always been designed for safety purposes as they interact with real-life aspects of the world with emphasis to safety rather than security. The demand to integrate industrial control system networks of an enterprise to the Internet have led to heterogeneous system designs and complex architectures, thereby, creating security vulnerabilities that are easy targets of cyber-attacks. Furthermore, if not properly deployed, they can be susceptible to attacks due to their legacy protocols and proprietary technology.

Industrial systems are part of the critical infrastructure of a nation and the US government has acknowledged their security risk. In 2001, as part of the ”Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism” Act of 2001 (USA PATRIOT Act), the US Congress passed the Critical Infrastructures Protection Act of 2001 ((CIPA) 42 US Code § 5195c Critical infrastructures protection) [1] directing the National Infrastructure Simulation and Analysis Center (NISAC) to support for the activities of the President’s Critical Infrastructure Protection and Continuity Board. The Act directed the NISAC to perform modeling, simulation and analysis of cyber and/or physical systems on the critical infrastructures to understand their complexity thereby assisting in suitable modifications to mitigate threats. In a written testimony from the NPPD office Assistant Secretary [2], external actors are targeting government entities and businesses in the energy, nuclear, water, aviation, and critical manufacturing sectors. In reality, there is still an increasing gap of skilled expertise in Industrial cyber-security starting at the academic level. A National Audit Office survey [3] in 2015 highlights the gap in cyber-security skills. Securing Critical Infrastructure is a specialized branch of traditional Cyber-security largely following the Critical Security Controls as prescribed by the Center for Internet Security (CIS) [4]. Few CIS controls for cyber defense preparedness are Penetration Tests and Red Team Exercises (CIS control #20) and Incident Response and Management (CIS control #19). Attackers often identify and exploit a gap between good defensive architecture and their implementation or maintenance.

In this paper, the authors describe the build of a low-budget, near-world, Supervisory Control and Data Acquisition (SCADA) testbed (laboratory) specifically designed for Industrial cyber-security research and industrial incident forensics research at SHSU.

II. Background

Existing ICS/SCADA testbeds are usually full-scale functional or small-scale physical models or primarily software-simulated models. The SCADA testbed program at Idaho National Laboratories (INL) [5] is a large scale design dedicated for ICS cyber security learning and trainings. Mississippi State University [6] and University of New Orleans [7] have built a small-scale physical testbeds for academic learning around Industrial Systems with a dual use for cyber-security. Thiago et al [8] examine the fidelity of a virtual SCADA testbed to a physical testbed wherein a study of the effects of cyber-attacks on both the systems is undertaken. Methods to gather information and utilize available tools and techniques to increase situational awareness to survive a malicious electronic attack on SCADA systems have also been highlighted [9]. Ahmed et al [10] discuss the challenges faced in protecting SCADA systems and conducting forensic investigations on them. Nicholson et al [11] had surveyed ongoing research and provide a coherent overview of the threats, risks and mitigation strategies in the area of SCADA security. In a

978-1-7281-2827-6/19/$31.00 ©2019 IEEE

classroom setting, Conklin et al [12] outline the types of SCADA laboratory designs. A learning approach for students on SCADA systems' vulnerabilities through experiments and hands-on exercises was discussed by Sitnikova et al [13]. For a game based approach on such exercises, Hewett et al [14] present an analytical game approach to analyze cyber-attacks on smart-grid SCADA systems. However, a literature vacuum exists around a playbook for SCADA testbed (laboratory) design framework coupled with laboratory exercises specifically focusing on cyber-security readiness (penetration assessment and testing, SCADA protocols analysis, vulnerability assessments), defensive and offensive security, risk analysis and Industrial/SCADA incident forensics. In this paper, the authors propose a laboratory design by incorporating many of the CIS [4] controls including incident forensics. The authors use a gaming approach for the teams as part of the laboratory exercises similar to the ICS cyber-security (301) trainings [15] conducted by ICS-CERT.

III. Problem Statement and need for a lab

In an industrial setup, SCADA and process control system vulnerabilities can increase from poor communications between enterprise IT and engineering teams leading to a lack of cyber security preparedness in industrial process sensors [16], [17]. This situation usually arises due to lack of cross-domain knowledge between these teams. This communication gap can be addressed by honing defensive security skills, awareness of SCADA and process control systems, knowledge of engineering designs involved and incident forensics for the IT team. In this paper, the authors primarily focus on the framework to design and construct an Industrial Control Systems Laboratory (ICS lab) for the purposes of cyber-security and incident forensic research on Industrial Systems and automation. Another reason for the ICS lab was accompanying security and digital forensic courses and education provided at Sam Houston State University (SHSU). This ICS lab would thus help students and researchers practice various red team, blue team and incident forensic exercises. A key goal of the ICS lab's design was to mimic a real-world industrial engineering design on a low budget.

IV. Lab Design

SCADA systems are often viewed as a specialty subject of industrial engineers and technicians rather than IT engineers. The ICS lab's design was broken into three phases; conceptual design, logical design and physical design. The conceptual design focus was on real-world scenario of machine configurations, operating systems and the choice of protocols to configure. The logical design focused upon the code snippets for the near-corporate websites, Human-Machine Interface (HMI) coding, programming of the programmable logic controller (PLC) and near-corporate databases. The physical design focus was on the hardware and wiring of PLCs. Fig. 1 shows the original physical design with PLCs and over-time the lab has been expanded to house additional PLCs.

Computer hardware was requested from the Computer Science Department (SHSU). The HMI software "Indusoft Web Studio V7.1, SP3" was procured from Indusoft [18] through an educational license. The SCADA automation hardware units were procured through vendor donations from Automationdirect [19] and Eaton [20]. A Eaton XC100 PLC and Direct06 PLC from Automationdirect were used in the ICS lab's design. The SCADA protocols simulators were available online for free downloads [24], [26]. Wireless access points, security camera and other hardware were acquired by the project team Fig. 2.

The HMI screens Fig. 3 were designed to implement an industry process. The concept of the HMI screen was about a fictious chemical manufacturing company "KAT Engineering and Chemicals" that used a periodic and timed manufacturing processes that if went awry, could cause a potential environmental disaster. The start and stop of process (batch processing of chemicals) was triggered with HMI programming. Even after a period of time, if the Red team finds it unsuccessful in penetrating the network and systems of "KAT Engineering and Chemicals", random tag values aligned to a certain defined timed logic would cause an environmental disaster visible on the HMI screen. This fictitious disaster caused by pre-programmed logic would stop the plant's functioning triggering incident response analysis steps by the forensic team. The logic with building such a design was to introduce a gaming concept for red teams, blue teams and the forensic teams. The same forensic team would also need to be involved when an environment disaster takes place to ascertain if the incident was related to a security breach. The ICS lab's architecture is designed such that it can be scaled up or down in equipment depending on the Industry needs and the proposed trainings.

A. Security Architecture

The overall security architecture design of the ICS lab was planned to mimic real-world design as found in many industrial enterprise IT ecosystem with industrial control systems. The network design involves hardware as below;

- Network Hardware: Palo Alto Firewall, Cisco and Tenda Router/Switches
- Honeypot toolbox for the lab instructors

All passwords were set to weak strength and were easy to crack. Files were randomly scattered on systems that gave away design details and other sensitive data. The security camera was positioned such that a hacker could view the HMI screen through its web interface. Passwords to machines were intentionally scribbled on paper and left around to mimic carelessness by real-world personnel. Keeping with ICS industry security hygiene [21], operating systems were lightly patched. The database tables had application passwords in plaintext.

B. Hardware Architecture

For the ICS lab's network, the design focus was modelled after generally found deployments in the Industrial world. The design involved no dedicated computers or servers for

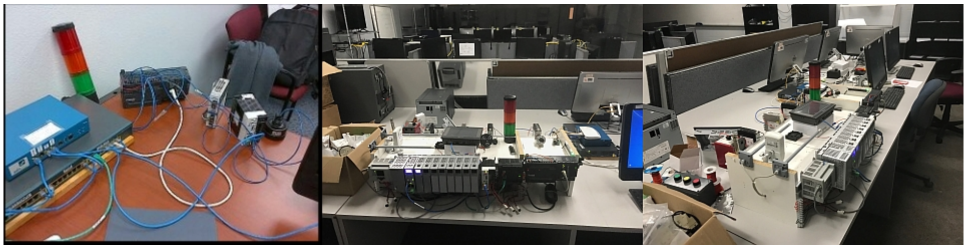


Fig. 1. Original Lab setup (left) and Current Lab setup of (center, right) Systems and Network

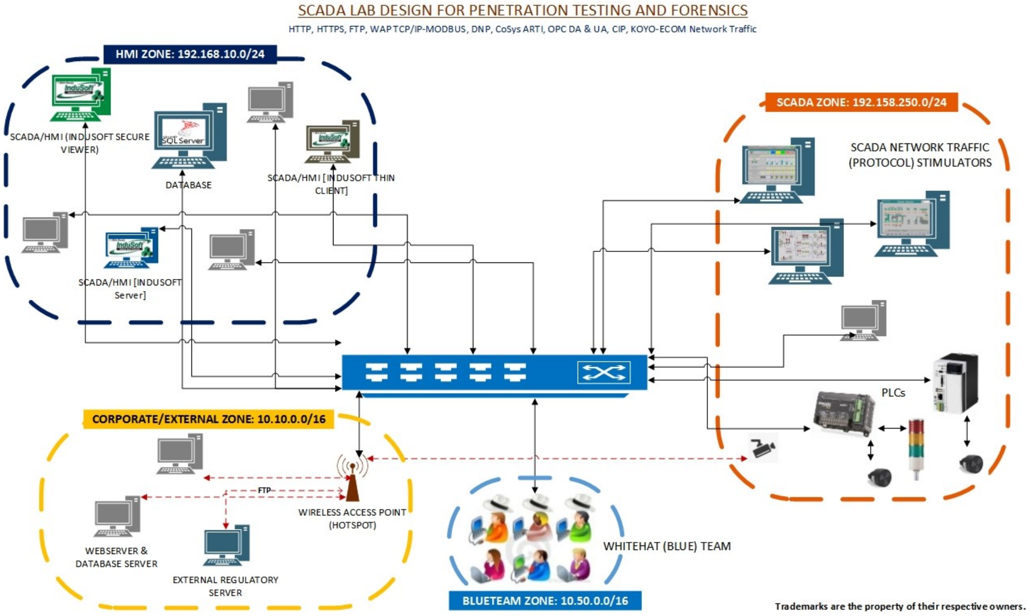

SCADA LAB DESIGN FOR PENETRATION TESTING AND FORENSICS
HTTP, HTTPS, FTP, WAP TCP/IP-MODBUS, DNP, CoSys ARTI, OPC DA & UA, CIP, KOYO-ECOM Network Traffic
HMI ZONE: 192.168.10.0/24
SCADA/HMI (INDUSOFT SECURE VIEWER)
SQL Server
DATABASE
SCADA/HMI [INDUSOFT THIN CLIENT]
SCADA/HMI [INDUSOFT Server]
SCADA ZONE: 192.158.250.0/24
SCADA NETWORK TRAFFIC (PROTOCOL) STIMULATORS
PLCs
CORPORATE/EXTERNAL ZONE: 10.10.0.0/16
FTP
WIRELESS ACCESS POINT (HOTSPOT)
WEBSERVER & DATABASE SERVER
EXTERNAL REGULATORY SERVER
WHITEHAT (BLUE) TEAM
BLUETEAM ZONE: 10.50.0.0/16
Trademarks are the property of their respective owners.

Fig. 2. Network Design

a purpose, no or minimum network firewalls, a combination of operating systems like Windows7, Windows2000, Windows2003 and WindowsXP [21]–[23]. This kind of design was determined to exist in any random small-sized Industrial unit's IT infrastructure that uses SCADA systems. For the SCADA hardware, few vendors had donated PLC's and accessories for the ICS lab. They were programmed for use. IP based security cameras and wireless routers are also part of the architecture as they can be mostly found in the IT design of Industries using SCADA systems

C. Software Architecture

The ICS and SCADA design of the lab had the following software. Some of the software have existing licensing agreements with SHSU and the rest are free for general use. The ICS protocols; MODBUS, TCP/IP, OPC-DA, OPC-UA, ARTI CODESYS, DNP3, KOYO, IEC 60870-5-104 and AB-DF1 were identified as needed after discussing with experts in the ICS this industry.

- Indusoft Web Studio and thin client [18]
- PLC Stimulation software ”ModRSSim” [24] for MODBUS protocol
- PLC Simulation software “Communication Protocol Test Harness” [25] for DNP3.0 and IEC 60870-5-104
- KepserverEx [26] for OPC

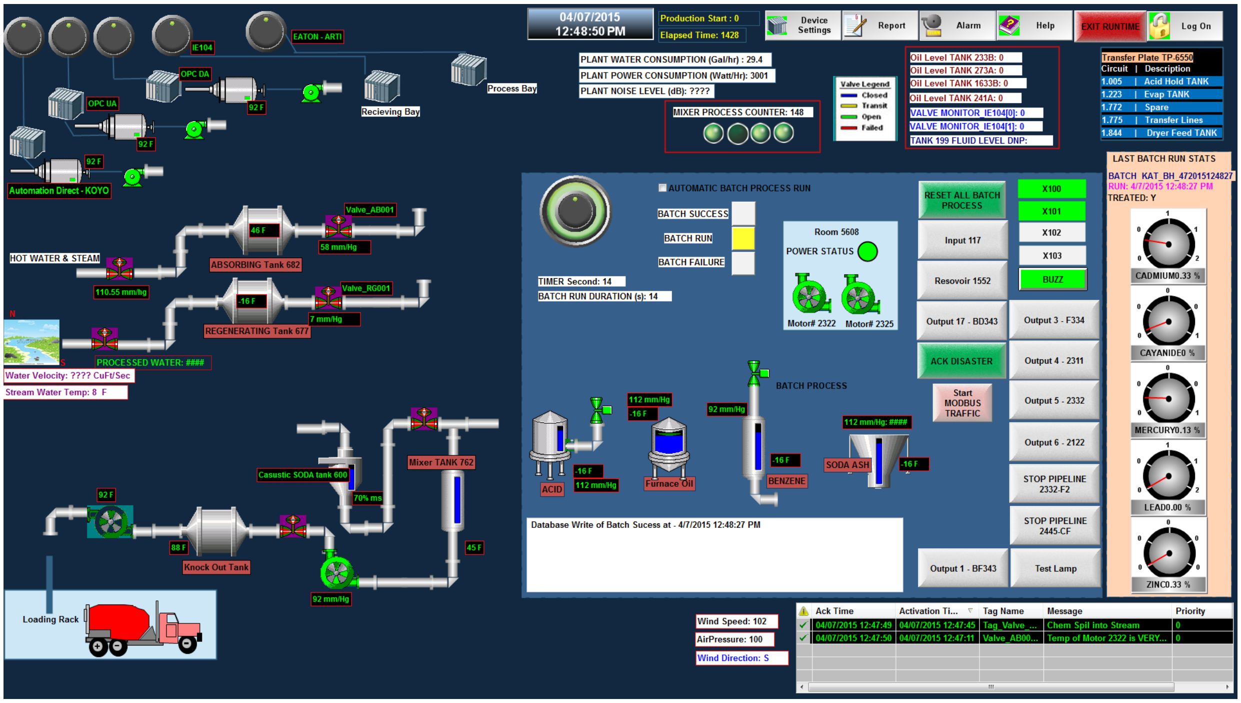
D. Database Architecture

Databases aid in SCADA data storage and in corporate application data storage scenarios. As databases are found at all industrial enterprises and are good targets for attacks, the addition of databases to the ICS lab design was needed. To mimic real-world cases of database versions at an enterprise, older versions of SQL Server were used. Following are the highlights of the database instances in the ICS lab's design;

- SQL Server 2000 and 2008 versions were installed on different Windows O/S machines.
- DB Instances have jobs and packages.
- Existence of mirror DBs and replication.
- Loose database security design (for honeypots).

E. Corporate DMZ

The addition of corporate systems and traffic helps in recreating any enterprise using Industrial controls. The corporate and DMZ design was segregated with firewalls. Automated application scripts were employed to generate network traffic.



Database Write of Batch Sucess at - 4/7/2015 12:48:27 PM

	Ack Time	Activation Ti...	Tag Name	Message	Priority
✓	04/07/2015 12:47:49	04/07/2015 12:47:45	Tag_Valve_...	Chem Spil into Stream	0
✓	04/07/2015 12:47:50	04/07/2015 12:47:11	Valve_AB00...	Temp of Motor 2322 is VERY...	0

Fig. 3. HMI Screen

Few task scheduler driven jobs for file transfer using FTP were deployed. The toolkit for attack, defense and incident forensics are below.

- Penetration-testing Tools - Wireshark, Metasploit, SQLMap, NETCAT, HPING
- Forensic Tools : Encase, FTK-pro
- Use of Cyber Vulnerability Assessments Tools, Kali Linux O/S
- ICS-CERT tools

F. Teams

The red team is a highly skilled group that assess security methodologies through reconnaissance, adversarial simulation and targeted attacks. Likewise the blue team consists of resources who dedicate their time in defending, hardening systems (patching), monitoring and securing the enterprise. The Incident forensic team specializes in evidence acquisition and management, documentation, chain-of-custody and forensic analysis of the security incident.

V. ICS Lab Set up

The ICS lab set up process started with the PLCs as they were received ahead of the project schedule. The PLCs were wired to the DC supply, stacklights, buzzers and programmed with tags that could be invoked from the HMI software (Indusoft). A few separate logic programs were also added to the PLCs to generate random LEDs bursts so that the units really looked functioning in a complicated way to the nonprofessional's eyes. Windows XP and Windows 2003 were setup as VMs and host machines were on Windows-7. All operating systems had a degree of minimal security patching [21]. The Palo Alto Firewall and Cisco switch were programmed in relation to the defined firewall zones. The desktops, VMs and PLCs were integrated with the Firewall and switch. The Wireless access point and the wireless security cameras were the last of the hardware to be integrated to the network. The SCADA protocol simulators were installed on the identified machines. A HMI screen was programmed with drivers invoking the simulators and PLCs. The HMI screen was also programmed to the SQL Server Database on the network. A separate SQL Server database was setup to mirror the primary database and also serve as an ad-hoc historian. Genuine and fake SQL Data Transformation Services (DTS) jobs were setup on the database servers to mimic a corporate design. The IIS webservers were configured for hosting corporate websites and FTP traffic. Few websites were created in classic ASP allowing SQL Injections. A few scheduled batch scripts were created to FTP files between machines. A ICS lab manual and courseware was developed covering introduction to Industrial control systems, current threats, defense tools and forensic challenges. A list of all known honeypots within this ICS lab was also documented. Details on the team skills needed (red, blue and forensics team) were also outlined on the training guide.

VI. Design Verification and Validation

Verification of the ICS lab functioning involved working with a toolkit that would normally be used for vulnerability testing, penetration testing and incident forensics by professionals. Many of these tools were open sourced or used from Kali Linux distro. Below are the verification and validation tasks performed and tools used.

- MODBUS protocol traffic - Wireshark
- OPC DA protocol traffic - Simulator logs
- OPC UA protocol traffic - Wireshark
- KOYO protocol traffic (KOYO is transmitted as UDP packets) - Wireshark
- EATON's CodeSYS ARTI protocol traffic - Simulator logs
- DNP 3.0 protocol traffic - Wireshark
- IE104 (IEC 60870-5-104) protocol network traffic - Simulator logs
- Direct06 PLC configuration - HMI alarms and logs
- Eaton PLC configuration - HMI alarms and logs
- Password strength test - John the Ripper
- Penetration tests against lab network - Metasploit
- Windows security patches to expose backdoors - Microsoft Baseline Security Analyzer
- SQL Injection against lab corporate websites - SQL Map
- Open and vulnerable ports against lab network - NMap
- Website vulnerabilities against lab network - Vega
- Forensic tools to acquire a disk image - Autopsy
- System and application logging - HMI Historian, Windows Logs, Syslog

VII. Lab Use Cases

The primary objective of this laboratory is for students to conduct experiments and understand the importance of Industrial control systems as cyber-targets. Few use cases of the ICS lab were identified for students. They were also the driving factors during ICS lab design considerations and core requirements in the project design phase. The ICS lab can be used as below during and off-training cycles;

A. Defensive Security

White Hat (blue) teams can use of the lab for practical experiments, study defensive methods and conduct research in areas like system hardening, implementing security industry best practices, vulnerability management etc.

B. Offensive Security

Black Hat teams (Red team) can use the ICS lab for offensive experiments, study of offensive methods and conduct research in the areas like Attack stimulation and Offensive testing (ICS lab validation).

C. Forensics study and research

SCADA forensic investigations are different from routine corporate network forensics or home network forensics due to the nature of industrial systems involved [10]. SCADA systems are not only dependent on safety but also on security [27]. ICS are not easily configurable for any forensic activity. Often ICS systems cannot be brought offline for forensic making it harder to conduct live forensics during post-analysis of a cyber-incident [28]. Users can conduct various live forensic investigations (network, file-system, volatile memory, PLC memory, time-synchronization) against true or staged incidents during training exercises and benefit from a near real-world ICS lab setting. A forensic investigation can help answer many questions such as;

- Was the SCADA systems compromised by a malware attack?
- Did the incident have a payload involved?
- Was there a command and control (C&C) traffic involved in the attack?
- Did an insider (SCADA operator) cause the incident?
- How to contain the incident?
- How to perform incident root-cause analysis?
- How to work with the engineering and security (blue) teams to investigate the incident?
- How to conduct live forensics with fragile systems?

D. Incident management

Often operations staff do not have the skills to collect and disseminate a cyber-incident and rely on vendor/integrators for support. This can delay incident analysis leading to loss of critical real-time data. Users can engage in an exercise detailing an incident response team's ability to respond to stimulated cyber incidents within the ICS lab. Such exercises would also help students better understand the importance of Intrusion Detection Systems (IDS), ICS-CERT and Security information and event management systems (SIEM).

E. Frameworks study and research

Security framework study and research by users as in the study of various ICS, NERC Industrial security frameworks and understand their implementation against the near real-world lab setting.

F. Industrial cyber-security

Students often limit their cyber defense knowledge due to the lack of a lab as a playground. Coupling corporate-type Internet facing systems with industrial systems gives students a real-world interface of computers and the importance in defending them. General aspects of system behavior monitoring, attack estimation and prevention, insider threats, known and unknown attack detection [29] can be studied in a lab setting.

G. Risk Management

Students can evaluate current risk mitigation procedures related to cyber-attacks and identify critical gaps in risk planning, develop appropriate risk mitigation controls and recommendations in response to the types of stimulated cyber-attacks on the lab.

H. Vulnerability Assessments

Students can use the ICS lab to conduct assessments for vulnerabilities. ICS-CERT's Cyber Security Evaluation Tool (CSET) [30] is vulnerability assessment tool that can be used to perform a self-assessment of the vulnerabilities found on the ICS lab's systems. This tool uses hybrid risk and standards-based approach to evaluate the cyber-security of an industrial control or business system to provide relevant recommendations for improvement. Care should be taken to trigger less intrusive vulnerability scans as some ICS devices may exhibit abnormal behavior due to such scans.

VIII. Conclusion

The ICS lab at SHSU serves as a unique testbed for students and researchers interested in Industrial Control Security and incident forensics. The ICS/SCADA hardware was limited to a few PLC's and accessories due to limited budget. Since the lab was initially setup, additional ICS/SCADA hardware has been included to allow for a more diverse ecosystem of industrial protocols and systems. A HTML5 browser capable mobile interface was initially planned but could not make it to the final design. In future upgrades of this lab, HMI mobility and industrial related Internet-of-Things (IoT) devices can be incorporated.

IX. Acknowledgment

A word of thanks to Automationdirect and Eaton for donating SCADA hardware. The authors thank Andre Bastos at Indusoft for his help with PLC programming, Tim McGuffin (Ex-Information Security Officer, SHSU) for his help with the network configurations and Andrew Bennett (Ex-Director, Center of Excellence in Digital Forensics, SHSU) for his support in obtaining the Indusoft Educational License.

References

[1] P. V. Domenici, "S.1407 - 107th Congress (2001-2002): Critical Infrastructures Protection Act of 2001," 2001. [Online]. Available: https://www.congress.gov/bill/107th-congress/senate-bill/1407

[2] Assistant Secretary Jeanette Manfra, "Written testimony of NPPD for a House Homeland Security Subcommittee on Cybersecurity & Infrastructure Protection and House Armed Services Subcommittee on Emerging Threats & Capabilities hearing regarding Interagency Cyber Cooperation — Homeland Security," 2018. [Online]. Available: https://www.dhs.gov/news/2018/11/14/written-testimony-nppd-house-homeland-security-subcommittee-cybersecurity

[3] "The digital skills gap in government: Survey findings," Cabinet Office, UK, Tech. Rep., 2015. [Online]. Available: https://www.nao.org.uk/wp-content/uploads/2015/12/The-digital-skills-gap-in-government-Survey-findings-December-2015.pdf

[4] "CIS Controls." [Online]. Available: https://www.cisecurity.org/controls/

[5] "Idaho National Laboratory." [Online]. Available: http://www.inl.gov/

[6] T. Morris, R. Vaughn, and Y. S. Dandass, "A testbed for SCADA control system cybersecurity research and pedagogy," in *Proceedings of the Seventh Annual Workshop on Cyber Security and Information Intelligence Research - CSIIRW '11*. New York, New York, USA: ACM Press, 2011, p. 1. [Online]. Available: http://dl.acm.org/citation.cfm?doid=2179298.2179327

[7] I. Ahmed, V. Roussev, W. Johnson, S. Senthivel, and S. Sudhakaran, "A SCADA System Testbed for Cybersecurity and Forensic Research and Pedagogy," in *Proceedings of the 2nd Annual Industrial Control System Security Workshop on - ICSS '16*. New York, New York, USA: ACM Press, 2016, pp. 1–9. [Online]. Available: http://dl.acm.org/citation.cfm?doid=3018981.3018984

[8] T. Alves, R. Das, and T. Morris, "Virtualization of Industrial Control System Testbeds for Cybersecurity," in *Proceedings of the 2nd Annual Industrial Control System Security Workshop on - ICSS '16*. New York, New York, USA: ACM Press, 2016, pp. 10–14. [Online]. Available: http://dl.acm.org/citation.cfm?doid=3018981.3018988

[9] J. Pack and Jeff, "Situational awareness for SCADA systems," in *Proceedings of the Fifth Cybersecurity Symposium on - CyberSec '18*. New York, New York, USA: ACM Press, 2018, pp. 1–2. [Online]. Available: http://dl.acm.org/citation.cfm?doid=3212687.3212865

[10] I. Ahmed, S. Obermeier, M. Naedele, and G. G. Richard III, "SCADA Systems: Challenges for Forensic Investigators," *Computer*, vol. 45, no. 12, pp. 44–51, dec 2012. [Online]. Available: http://ieeexplore.ieee.org/document/6298895/

[11] A. Nicholson, S. Webber, S. Dyer, T. Patel, and H. Janicke, "SCADA security in the light of Cyber-Warfare," *Computers & Security*, vol. 31, no. 4, pp. 418–436, jun 2012. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167404812000429

[12] P. J. Conklin Wm. Arthur, "Design of a SCADA laboratory to support IT Classes," in *Proceedings of the 15th Colloquium for Information Systems Security Education*, Fairborn, Ohio, 2011. [Online]. Available: https://www.researchgate.net/profile/Jenifer_Amla/post/How_to_develop_SCADA_in_laboratory_environment/attachment/59d63dac79197b807799a705/AS%3A420967135367169%401477377794728/download/65.pdf

[13] E. Sitnikova, E. Foo, and R. B. Vaughn, "The Power of Hands-On Exercises in SCADA Cyber Security Education." Springer, Berlin, Heidelberg, 2013, pp. 83–94. [Online]. Available: http://link.springer.com/10.1007/978-3-642-39377-8_9

[14] R. Hewett, S. Rudrapattana, and P. Kijsanayothin, "Cyber-security analysis of smart grid SCADA systems with game models," in *Proceedings of the 9th Annual Cyber and Information Security Research Conference on - CISR '14*. New York, New York, USA: ACM Press, 2014, pp. 109–112. [Online]. Available: http://dl.acm.org/citation.cfm?doid=2602087.2602089

[15] "CERT - Training Available Through ICS-CERT — CISA Cyber Infrastructure." [Online]. Available: https://ics-cert.us-cert.gov/Training-Available-Through-ICS-CERT{\#}workshop

[16] "Information Security Principles for Business Resilience," Tech. Rep., 2012. [Online]. Available: https://www.tisn.gov.au/documents/itseag+secure+your+information+cio.pdf

[17] J. Weiss, "A Grim Gap: Cybersecurity of Level 1 Field Devices and lack of appropriate OT Expertise," 2019. [Online]. Available: https://www.controlglobal.com/blogs/unfettered/a-grim-gap-cybersecurity-of-level-1-field-devices-and-lack-of-appropriate-ot-expertise/

[18] "InduSoft Web Studio HMI SCADA Development Software." [Online]. Available: http://www.indusoft.com/

[19] "AutomationDirect - Home." [Online]. Available: https://about.automationdirect.com/

[20] "EATON." [Online]. Available: https://www.eaton.com/us/en-us/company/about-us.html

[21] D. Z. Kapellmann, N. Brubaker, and R. Caldwell, "ICS Tactical Security Trends: Analysis of the Most Frequent Security Risks Observed in the Field," 2018. [Online]. Available: https://www.fireeye.com/blog/threat-research/2018/10/ics-tactical-security-trends-analysis-of-security-risks-observed-in-field.html

[22] B. Contos, "Security Instrumentation for Industrial Control Systems (ICS) Environments," 2018. [Online]. Available: https://www.verodin.com/post/security-instrumentation-for-industrial-control-systems-ics-environments

[23] S. Mallur, "Demystifying Cyber Security in Industrial Control Systems." [Online]. Available: https://www.isaca.org/Journal/archives/2017/Volume-4/Pages/demystifying-cyber-security-in-industrial-control-systems.aspx

[24] "Modbus PLC Simulator." [Online]. Available: http://www.plcsimulator.org/

[25] "Communication Protocol Test Harness, Triangle Microworks Inc." [Online]. Available: http://www.trianglemicroworks.com/products/downloads

[26] "KEPServerEX Connectivity Platform — OPC Server — Kepware." [Online]. Available: https://www.kepware.com/en-us/products/kepserverex/

[27] M. Brändle and M. Naedele, "Security for Process Control Systems: An Overview," *IEEE Security & Privacy Magazine*, vol. 6, no. 6, pp. 24–29, nov 2008. [Online]. Available: http://ieeexplore.ieee.org/document/4753670/

[28] F. Adelstein and Frank, "Live forensics," *Communications of the ACM*, vol. 49, no. 2, p. 63, feb 2006. [Online]. Available: http://portal.acm.org/citation.cfm?doid=1113034.1113070

[29] Q. Chen and S. Abdelwahed, "Towards realizing self-protecting SCADA systems," in *Proceedings of the 9th Annual Cyber and Information Security Research Conference on - CISR '14*. New York, New York, USA: ACM Press, 2014, pp. 105–108. [Online]. Available: http://dl.acm.org/citation.cfm?doid=2602087.2602113

[30] "Cyber Security Evaluation Tool (CSET): Performing a Self-Assessment," 1969. [Online]. Available: https://www.hsdl.org/?abstract&did=695539