Design of a SCADA Laboratory to Support IT Classes

Wm. Arthur Conklin, *University of Houston*, and Jonathan Pollet, Joe Cummins, *Red Tiger Security*

Abstract

Computers have controlled physical systems for decades, but increasingly today, these systems are being interconnected to enterprise IT systems via the Internet. The reasons revolve around efficiency, but the practical matter is that IT personnel are encountering these non-standard IT systems and must learn to integrate them into their operational world. To introduce students to the world of SCADA networks and protocols, together with the operational and security requirements, a laboratory facility is designed and constructed with accompanying curriculum.

Index terms – SCADA, Security, Security Laboratories, Curriculum

I. Introduction

This paper describes to design and integration of a SCADA laboratory into an IT curriculum at both the undergraduate and graduate level. The laboratory is also designed to support both basic research and community outreach efforts to local industry partners. Although located in a university information security center, the lab also supports basic understanding efforts associated with IT education efforts.

SCADA is often viewed as a specialty subject, more the venue of engineers and technicians than standard IT personnel. Over the past several decades, as cyber-physical systems have spread and are now moving to use the Internet for purposes of connectivity, the separation between the SCADA and IT communities has vanished. Protocols that were once only of concern to SCADA technicians are now being seen in network traffic across a wide range of networks. The computer based control of physical devices is not isolated to industrial processes, but are in many different venues, including transportation, building environment controls, energy, manufacturing (big and small), and logistics/distribution. The widespread use of electronic controllers using the Internet for connectivity makes the understanding of this type of network and network traffic an increasingly important area of IT education.

From a security point of view, these newly connected systems pose several threat opportunities [1]. One threat opportunity is an attack to the devices under control. Another threat avenue is an attack on the enterprise under the cover of the new, non-standard, network associated with the control systems. For students to learn how these systems work and how to integrate SCADA and regular enterprise IT networks requires exposure to these concepts. Exposure can be in the form of lecture elements, or hands-on work. Hands-on learning has been shown to be more effective in learning and integrating advanced concepts. Having a lab to support this type of learning increases the utility offered by an information security program to students and the firms that ultimately employ them.

This paper is organized as follows; an examination of what SCADA systems are is followed by a description of the lab design. The curriculum related elements that are supported by the lab is presented next, followed by future research directions and opportunities.

II. SCADA

SCADA is an acronym for Supervisory Control and Data Acquisition. This is an acronym that is used in a general sense to cover a wide range of cyber-physical systems. Each industry has its own naming methodology for the systems and components associated with the remote computer control of physical equipment. These computer systems are distributed across the physical systems they control. The terms distributed control systems (DCS) and industrial control systems (ICS) are also used to refer to these systems. For the purposes of this paper, we use the term SCADA to refer to all of these distributed systems.

The different types of SCADA systems, whether they are ICS, or DCS, and depending upon the system they are controlling perform different functions. Historically, DCS based systems tend to be process oriented, while SCADA systems tend to be data gathering oriented. Today, with the use of information to improve processes, the lines between data gathering and data usage for process control are blurring. These systems need reliable communications over potentially slow and unreliable

Wm. Arthur Conklin, University of Houston, College of Technology, waconklin@uh.edu, and Jonathan Pollet, Joe Cummins, Red Tiger Security.

ISBN 1-933510-96-X/$15.00

channels. SCADA systems are comprised of several components and their own network structure with corresponding specialized protocols to allow communication. These elements are then connected to the enterprise network via standard TCP/IP protocols.

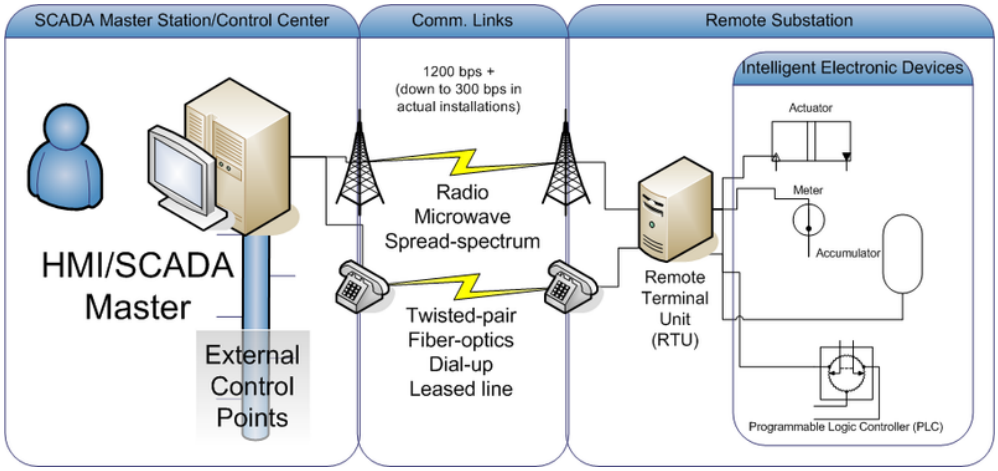

Figure 1. Typical SCADA system and communications[2]

The standard elements of a SCADA system include programmable logic controllers (PLC), remote terminal units (RTU), intelligent electronic devices (IED) and human machine interfaces (HMI) [1]. An additional software element is the data historian, a centralized database to keep track of all of the data associated with the system. The PLC is a device that is programmed to perform the basic logic functions associated with the physical system under control. Various sensors and switches can act as inputs and other switches act as outputs from the logic program. PLCs are an economical method of implementing logic functions into the control of physical processes and their programs can be quite complex in modern systems. An RTU functions to gather data from distant sensors, typically through a distributed communication network, such as a radio network. An IED can be used for basic measurement and control. All of these devices are integrated together and controlled via a software program referred to as the HMI. The HMI allows an operator the ability to monitor the control functions being implemented by the control system.

Different industries can have different names and nomenclatures for the devices. The electric industry refers to its control system as the smart grid, although this term has additional meaning in the final delivery of electricity to customers. Across the transmission and distribution system, switches and relays are controlled via control circuits to regulate the follow of energy. The names of the elements are changed, but the end function is the same, computer control over physical infrastructure.

The purpose of the laboratory is to introduce students to the concepts and functions associated with these systems. For that reason, a generic setup is employed, placing the focus on the general nature of these control devices and their communication methods, leaving the industry specific language for classroom exploration at a different time.

Although different manufacturers have implemented protocols in different manners, including proprietary protocols, the lab is structured around two common protocol sets, Modbus and DNP3. The Modbus protocol is the most common SCADA protocol and is widely used to pass messages to SCADA equipment [3]. The DNP3 protocol is widely found in electrical and water systems, but tends to be scarcely used in other infrastructures.

Cyber-physical systems, whether referred to as SCADA, ICS or DCS, are becoming increasingly more common in enterprise IT operations portfolios. These systems have been propagated all over manufacturing, industrial systems, transportation, energy and utilities to control the critical infrastructures that we use every day. The connecting of these systems to the Internet makes them a new challenge for corporate IT shops. While the engineering and technicians associated with each system are concerned with the purpose and function of the system to specific process goals, the IT and network ships have to be concerned with data connectivity and transport. In this regard, the differences between the various types and operational purposes of the system are minor at best and the challenge of maintaining good connections to non-standard IT equipment becomes a significant issue.

ISBN 1-933510-96-X/$15.00

III. LAB DESIGN

The laboratory serves as a focal point to enable learning associated with a wide range of SCADA type devices. To facilitate this breadth, a small-medium-large design concept was employed. This concept is instantiated through the development of different work areas, each with the resources associated with a different size of experimental environment. The small environment is extremely limited in scope; allowing focus on a narrow range of activities, while at the other end of the range, the large environment is a simulation of a complete enterprise which enables virtually any level of experiment.

The small lab environment consists of a PLC type device and associated elements under control. Direct or wireless connection to this simple form of device allows focused work centered on issues associated with protocols and device logic. This simplified setup removes many of the extraneous network and control system elements allowing initial and focused work on the act of control at the actual controller element. Figure 2 depicts a small environment setup, including an instrumentation machine designed to capture all of the network traffic to and from the device to allow analysis of the communication and responses.

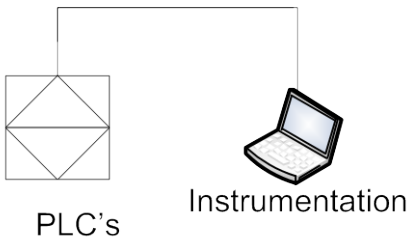

Figure 2. Small Lab Setup

The small lab environment is specifically designed to allow access to the SCADA protocols used to control devices on the SCADA network. Access at this level of granularity allows study of the component operation free form outside distraction. The primary targets of attack and threat vectors that can be analyzed with the small setup include those associated with the PLCs and other specific SCADA equipment. In the laboratory environment, a selection of different PLCs, RTUs and communication elements, including wired and wireless are available for experimentation. As Ethernet and TCP modules become more widespread, the addressability of these individual components over open networks such as the Internet has become a possibility, one that is governed by configuration of equipment and networks. This level of laboratory environment allows focused work into specific aspects at this level of granularity.

The medium lab setup, shown in Figure 3, adds an HMI interface and other control room type elements, such as a local data historian. This enables learning experiences associated with the control room element of a SCADA environment. This setup provides a richer SCADA experience and mimics much of what was once connected to enterprises via leased lines and other communication channels. The inclusion of the HMI and other control room elements makes this environment a complete operating environment from a cyber-physical point of view.

The range of operational experiments available to the medium environment is all of the work available in the small environment, with the addition of new items specific to the additional components. The inclusion of the additional elements makes some of the trivial exercises in the small environment less trivial as the interaction of higher level components in the overall SCADA system design begins to influence the system responses to various stimuli. This laboratory environment allows exploration of how the various SCADA components can work together as a system, and how these elements interact with respect to network behaviors.

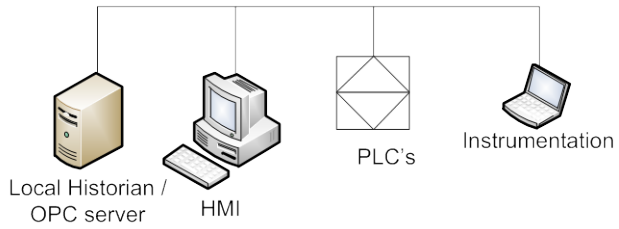

Figure 3. Medium Lab Setup

The large SCADA laboratory environment consists of three networks combined by firewalls; internal corporate enterprise network, a DMZ network, and a cyber-physical control network. These are illustrated in Figure 4. This environment is designed to allow the demonstration of complete interactions between a complex SCADA network and the SCADA system owner's corporate enterprise IT network. For reasons of operational efficiency, corporations have been connecting these separate networks, moving data back and forth between the operational SCADA network and the enterprise IT network.

The range of operational experiments available to the large SCADA environment is all of the work available in the small and medium environments, with the addition of new items specific to the additional components. The addition of a complete corporate IT environment, including network segregation, brings significant additional aspects for study. The inclusion of the additional elements makes some of the trivial exercises in the small and medium environments less trivial as the interaction of higher level components in the overall

SCADA system design begins to influence the system responses to various stimuli. This laboratory environment allows exploration of how the various SCADA components can work together as a system, and how these elements interact with respect to network behaviors. This comprehensive setup also facilitates more interesting information security work as the interaction of different protocols and the sensitivity of SCADA operations to certain external influences becomes observable and measurable.

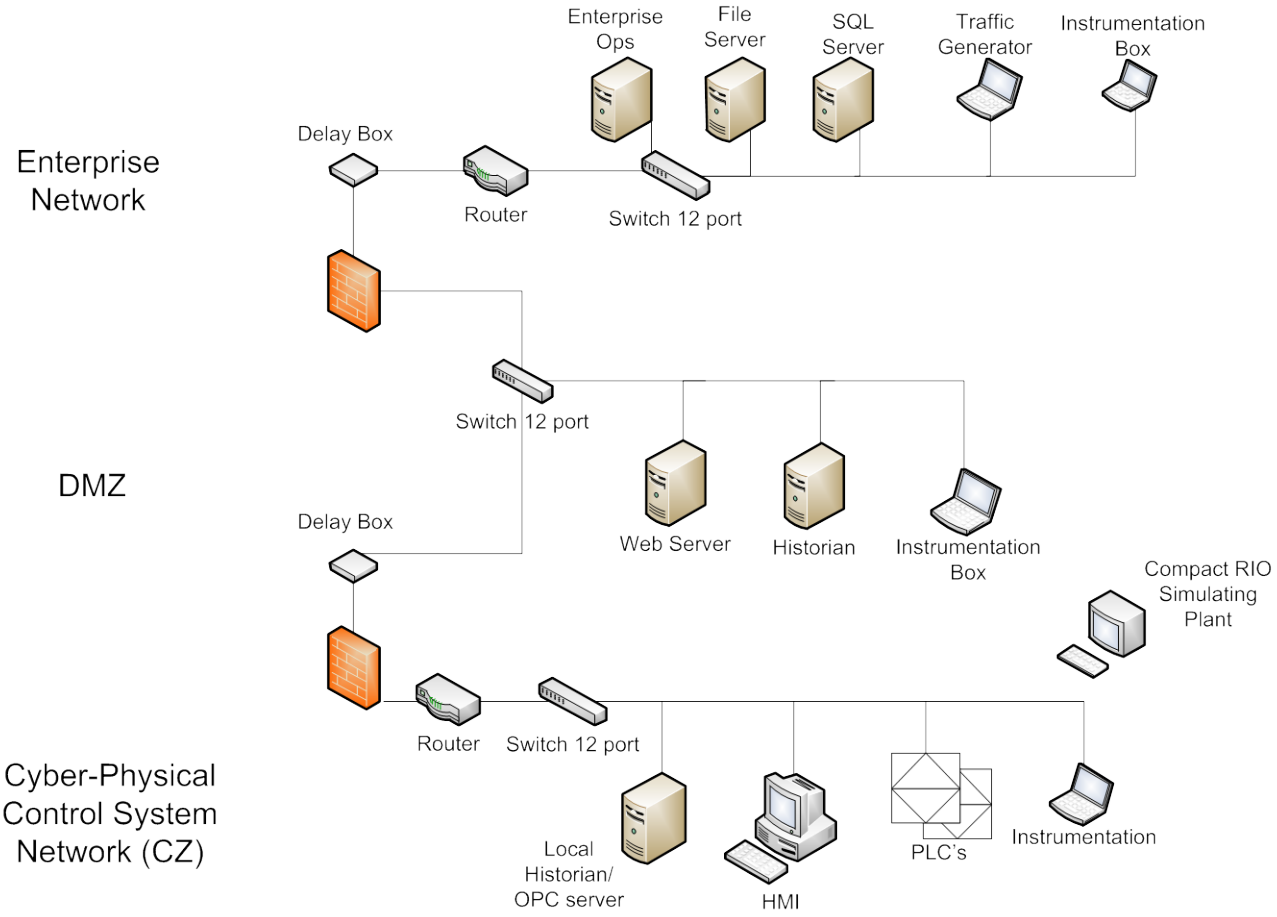

Figure 4. Large SCADA Setup

The integration of the enterprise IT element in the laboratory increases the complexity for several types of issues. Traffic based issues, such as intrusion detection, are trivial in the small setup, and become demanding and challenging in the large SCADA setup. The increase in numbers of protocols and types of communications makes security functions like IDS significantly more complex [4]. Issues such as security are also complexity driven and the added complexity to the enterprise network by including the SCADA network has significant effects on the security implementations across the enterprise [1, 5].

The configuration of the three environments is completely user definable. All of the equipment is co-located in a single room, including monitoring and interface equipment. To permit monitoring of the system, a series of workstations with monitoring software, connected to large displays is available to students and researchers. To facilitate realistic study of actual equipment found in the field, a selection of individual brands of equipment is available. This allows the selection of specific manufacturer's equipment to more closely replicate actual operating environments found in real-world settings. It is also designed so that the same equipment can begin as a small system setup, and with subsequent addition of components, become a medium sized deployment or even a large scale deployment. This allows experiments to grow organically through the full range from individual piece of equipment under study to an entire enterprise.

The development of a mix and match approach allows better interaction with local experts in the equipment and

operation of these systems and the faculty and student base. Engaging local industry personnel has multiple positive effects. First, the interactions with the students creates a better learning environment as it is based on actual lessons learned as opposed to what is in the textbook. The second important aspect is in the area of transitioning from student to employee. In this regard, the interactions in many ways replicate those of an internship. The company gets to see bright new minds still fresh in school and the students get to see what the real-world looks like with respect to potential career fields.

Engaging local industry in the laboratory also assists the research efforts in focusing on real problems that need to be solved. As one can imagine, with a system this complex, there are numerous topics and issues that can be the focus of research in these complex systems. Aligning research objectives with issues that are of direct concern to the system owners and operators will increase the chances of funding associated with the research.

IV. CURRICULUM

Laboratories can serve several purposes on a campus, and the SCADA laboratory is no different. One activity that it supports is research into actual cyber-physical control systems, from a design and operational point of view. Another is to support security studies associated with examining how to apply information security to these systems, protecting the valuable information and operations associated with these systems.

The primary purpose of this laboratory is to support student learning through hands on experimentation. To utilize the laboratory in classroom based learning requires integration with the classroom curriculum. Efforts are just beginning in this aspect, with the first steps being the introduction of various components and protocols in existing classes. For example, in the networking class where traffic is examined using Wireshark, a network packet monitoring program, the large SCADA setup provides traffic opportunities from not only a full enterprise, including email, web traffic, database and file servers, but also from specialty elements such as SCADA protocols over TCP, HMI and data historian traffic.

Security classes that examine issues such as updates can explore how mandated update strategies affect non-standard environments such as the SCADA network and its corresponding equipment. Having students observe a system fail because of common network scanning, when performing simple security testing, is a learning experience best performed in the lab during class, rather than on the job at their first job after their classroom education. SCADA systems, by their operational nature have some unique security requirements [1]. Examining how common security items, such as firewalls and IDS systems interact with these non-standard network systems is also a rewarding addition to a security professional's education.

The real strength of the laboratory setup in an educational environment comes not just from adding familiarization aspects into existing courses, but in the development of in-depth learning experiences associated with SCADA and IT. The Department of Homeland Security has commissioned a model curriculum in Control Systems Security which is designed to provide an educational exploration of the technical, managerial, economic and public policy aspects of SCADA systems [6]. This curriculum is designed to explore the risks associated with critical infrastructure elements and the efforts to secure them in an interdisciplinary manner [7]. The DHS curriculum is a high-level, management oriented curriculum, with no specific requirement for hands-on applications on actual SCADA systems.

The laboratory goes beyond this level of education, adding the technical hands-on aspect of forensic analysis [8], incident response [9], security architecture and other essential elements of secure infrastructure deployment. Having actual equipment on an instrumented test range will support active learning and provide students with a better understanding of the issues associated with these non-standard IT network elements. This setup will also facilitate and foster innovative thinking that is the impetus behind student and faculty research efforts, and provides the environment for knowledge discovery in this technical area.

V. FUTURE RESEARCH

Developing the laboratory and the initial curriculum is really just the first step in a long journey. As a wise philosopher once stated, happiness is not a destination, but a manner of travel, this laboratory provides us with a new means of travel, one that is a richer technological experience for students and faculty. The lab is designed to be modular, permitting the addition of new elements, and the reconfiguration of existing ones on a regular basis.

From a technological basis, there is room for additional types of equipment, especially in the wireless, 900MHz and Zigbee environments. Additional types of PLC, RTU and other equipment items can easily be incorporated, broadening the base of fielded systems that are cover via the laboratory environment. From a curriculum viewpoint, the implementation of the DHS model curriculum as a stand-alone element that can be deliver to the local energy industry is an area of potential growth.

On the research from, the laboratory setup provides a gold mine of opportunities. From protocols to system level

interactions, the world becomes available to researchers as the hardware is interchangeable, the software element is all instantiated via VMs, and hence rapidly reconfigurable. The most important element in all of the future activities is the connection between the lab and local industry. Their expertise and knowledge can provide insight and clarity as to where focus would be most productive. The challenge is in building these relationships, so that the information is made available to the researchers. With this guidance, the outcome will have a much greater chance of contributing to the resolution of important critical infrastructure elements issues.

VI. References

[1] K. Stouffer, J. Falco, and K. Scarfone, "NIST Special Publication 800-82: Guide to Industrial Control Systems (ICS) Security," *Gaithersburg, MD: National Institute of Standards and Technology (NIST),* 2008.

[2] Lemaymd, "Overview of the components in a typical DNP-connected SCADA system," DNP-overview.png, Ed., ed, 2005, pp. Image released to the public domain, no copyright.

[3] Modicon Inc., "Modicon Modbus Protocol Reference Guide," ed. North Andover, MA: Modicon, 1996.

[4] S. Hennin, "Control System Cyber Incident Reporting Protocol," in *Technologies for Homeland Security, 2008 IEEE Conference on*, 2008, pp. 463-468.

[5] Joint Task Force Transformation Initiative Interagency Working Group, "Recommended Security Controls for Federal Information Systems NIST SP 800-53 rev 3," ed. Gaithersburg, MD: National Institute of Standards and Technology 2009.

[6] P. Auerswald, L. M. Branscomb, S. Shirk, M. Kleeman, T. M. L. Porte, and R. N. Ellis, "Critical Infrastructure and Control Systems Security Curriculum," Department of Homeland Security, Ed., Version 1.0 ed. Washington, DC, 2008.

[7] R. Ellis, "Critical Infrastructure and Control Systems Security: An Interdisciplinary Approach," in *Technologies for Homeland Security, 2008 IEEE Conference on*, 2008, pp. 459-462.

[8] M. Fabro and E. Cornelius, "Recommended Practice: Creating Cyber Forensics Plans for Control Systems," *Department of Homeland Security,* 2008.

[9] Department of Homeland Security, "Recommended Practice: Developing an Industrial Control Systems Cybersecurity Incident Response Capability," *Department of Homeland Security,* October 2009 2009.