International Journal of Information & Network Security (IJINS)
Vol.1 No.4, October 2012, pp. 265~274
ISSN: 2089-3299

Portable SCADA Security Toolkits

Guillermo A Francia III*, Nourredine Beckhouche, Terry Marbut**, and Curtis Neuman****
*Mathematical, Computing, and Information Sciences Department, Jacksonville State University
**Department of Technology and Engineering, Jacksonville State University

Article Info

Article history:

Received Jul 20th, 2012
Revised Aug 10th, 2012
Accepted Sept 15th, 2012

Keyword:

SCADA
Cybersecurity
Toolkit
Security Education
Control Systems

ABSTRACT

The Internet and the demands of connectivity and convenience to access the control systems found in critical infrastructures have ushered newly discovered vulnerabilities that have been exploited by internal and external threats. These vulnerabilities of control systems could be exposed by even novice hackers through the use of non-sophisticated tools found on the Internet. These insecurities have been perpetuated by technology staff and even educators who are themselves unaware of the potential risks and consequences. This is further exacerbated by the lack of training tools and systems for the information security curriculum. We describe a cost-effective way of equipping educators with hands-on toolkits that can be used in their classrooms as security testing and learning kits. In addition, we describe several SCADA security curriculum modules that can be used for providing hands-on laboratory exercises utilizing the toolkits. We believe that this small contribution towards training future control system security professionals will have a tremendous impact on the security of industrial systems.

Corresponding Author:

Guillermo A Francia III
Mathematical, Computing, and Information Sciences Department
Jacksonville State University
700 Pelham Rd N, Jacksonville, AL 36265 USA
Email: gfrancia@jsu.edu

1. INTRODUCTION

The nation's critical infrastructure finds itself increasingly vulnerable to internal and external threats [5]. One of the most neglected aspects of critical infrastructure is the security of control systems, leading to very dangerous weaknesses that could be exposed by even novice cyberterrorists [7]. These insecurities are perpetuated by technology staff and even educators who are themselves unaware of the potential threats and their remedies [4, 6]. The need for information assurance and security education is well established. The ACM/IEEE's Computer Science Curriculum update in 2008 clearly identifies security as a major concern among emerging trends in the discipline [1]. A curriculum model on critical infrastructure (CI) and control systems security is described by Auerswald, et al. [2]. Although the model is characterized as interdisciplinary, it is mostly slanted towards the managerial and public policy aspects of the systems. In [3] an outline of the design and implementation of critical infrastructure and control systems, security course modules are presented. Although the course modules can be used to augment an existing course in CI, they can also be utilized as building blocks with which a complete CI security course could be built. We describe a cost-effective way of equipping educators with hands-on toolkits that they can use in their classrooms as both security testing and learning kits. Our vision is to augment these curriculum modules with the laboratory toolkits that are described in this paper.

1.1 PLCs, RTUs, and SCADA

Programmable Logic Controllers (PLCs) are a very popular and powerful controller. They are used in many of today's industries, hospitals, shopping centers, and amusement parks. They not only perform control functions for an automated system but can also exchange information with other controllers or PCs. Similar to PLCs, remote terminal units (RTUs) can also perform control functions and exchange information. However, the primary difference between the two is that PLCs are built to focus more on plant floor automation functionality whereas RTUs are built to focus more on remote communication functionality. As a result, an RTU will typically do a better job than a PLC at wirelessly communicating over long distances while a PLC will typically run an automation process faster than an RTU. A SCADA system is used to monitor and supervise an overall process being implemented by individual automated systems. It typically consists of the following four items:

- A master terminal unit (MTU), which is the central server where information about the overall process is collected. This allows a centralized workstation operator to monitor, analyze, and control the entire process from a remote location.
- PLCs and/or RTUs, which control the field equipment doing the process.
- Communications equipment for transferring data between the PLCs/RTUs and the MTU.
- Human machine interface (HMI) software, which enables the on-screen operation of the inputs (without physically touching them) and displays the status of the outputs. The HMI is installed on all workstations (including the MTU), allowing the operators to have easy and intuitive control over the systems.

1.2 Communication Protocols

Leading manufacturers of control systems include, among others, Rockwell Automation, GEFanuc, Modicon (Schneider Electric), and Siemens. These companies provide a variety of communication protocols, such as Modbus, Profibus, DeviceNet, Distributed Network Protocol 3 (DNP3), and Common Industrial Protocol (CIP) that are used to facilitate the efficient operations of control system hardware. The following subsections briefly describe each of these protocols.

1.2.1 Modbus Protocol

The Modbus protocol was developed by Modicon (Schneider Electric) for process control systems. Currently, it is the most utilized industrial communication protocol. The mode of communication is made through the master/slave primitive. Communication is made in units of transactions which can only be initiated by the master. A transaction type is either a query, response, or broadcast. The Modbus protocol provides communication error checking through character framing, parity check and cyclic redundancy check (CRC) [19].

1.2.2 Profibus Protocol

Profibus (Process Fieldbus) is an open standard and is based on a token bus/floating master system [19]. It is implemented as a three-layer protocol comprised of the Application Layer, the Data Link Layer, and the Physical Layer. The Application Layer typically handles three types of communication modes: the Fieldbus Message Specification (FMS) for complex messages, the Decentralized Periphery (DP) for universal messaging and faster delivery, and the Process Automation (PA) for intrinsically safe devices.

1.2.3 DeviceNet Protocol

DeviceNet serves as a communication network between industrial controllers and I/O devices. In order to complete its function enabling communication between nodes, it is built with the Common Industrial Protocol (CIP) on the upper network layers and the Controller Area Networking (CAN) standard on the data link layer [22]. DeviceNet supports three types of messages: explicit request/response messages, peer messages between two DeviceNet nodes, and I/O messages carrying predefined I/O data [20].

1.2.4 DNP3 Protocol

The DNP3 protocol is an open and public protocol. It is based on the International Electrotechnical Commission (IEC) Technical Committee 57 standards [17]. DNP3 is a simplified three-layer protocol. The three layers are the Physical Layer, implemented either through a serial RS-232/RS-485 or through an Ethernet connection; the Data Link Layer, which provides the error control mechanism and the logical link between sender and receiver; and the Application Layer, which includes a pseudo-Transport Layer that segments the messages into multiple data link frames. Application Layer messages are typically requests for operations and responses to corresponding requests [18]. The Physical Layer is implemented either through a

serial RS-232/RS-485 or through an Ethernet connection. The Data Link Layer provides the error control mechanism and the logical link between sender and receiver. The Application Layer includes a pseudo-Transport Layer that segments the messages into multiple data link frames [18]. Application Layer messages are typically requests for operations and responses to corresponding requests.

1.2.5 Common Industrial Protocol

The Ethernet/Industrial Protocol (IP) network is configured by layering the Common Industrial Protocol (CIP) over the standard protocols used by the Internet (Transmission Control Protocol (TCP)/User Datagram Protocol (UDP) and Internet Protocol (IP)) [21]. The Common Industrial Protocol is jointly managed by the Open DeviceNet Vendors Association (ODVA) and ControlNet International. It facilitates the integration of I/O controls, device configuration and data collection across multiple networks [23]. The rest of the paper is organized into five sections. First, we provide a literature review of a representative sampling of Supervisory Control and Data Acquisition (SCADA) training systems. Next, we describe the design and implementation of the two training kits that we developed. Third, we list the curriculum modules that are designed to accompany the toolkits. Fourth, we describe the pedagogical materials and activities that we are currently developing for the associated toolkits. Finally, we conclude the paper with some learning and teaching insights and also outline possible future work extensions.

2. RELATED WORK

The Tofino SCADA Security Simulator [13] is a portable and complete SCADA system that can be used for research and training on SCADA and PLC component vulnerabilities. The self-contained solution uses real-world PLC components and Human Machine Interface (HMI) to demonstrate SCADA operations on a highly realistic industrial scenario. CYBATI [8] promotes a Laboratory Research Kit in conjunction with their three day hands–on cyber security course. The kit features either an Allen Bradley Micrologix 1100 or Siemens S7-1200 programmable logic controller. Commercially available HMI software is utilized and license files are provided through a USB dongle. The system includes either routable network communications with Programmable Controller Communication Commands (PCCC) or Profibus- depending on the controller. Linux Backtrack 4 R2 is used as the virtual machine for the trainer. This system allows hands-on exercises involving basic PLC programming, security assessment, HMI development, analysis of communications, and attack analysis of PLC, HMI, and/or communications channels.

Another commercially available trainer uses the demonstration version of InTouch WONDERWARE [9]. The 32 tag maximum associated with the demo version is somewhat limiting but acceptable for basic SCADA training. An analog and a digital SCADA module, as well as an RS232 to RS485 converter used to connect those modules to the computer running the software, are provided as part of the trainer. The analog module has six bi-polar and two uni-polar inputs with five potential voltage levels. The limitation is that all inputs must operate at the same level. When the computer sets a voltage level for analog inputs, that level applies to every input. The module does have internal voltages available to simulate signals as well as terminal connections for utilization of external inputs. The final module provided with the trainer is for digital signals. The module has seven inputs and eight, open collector outputs. Again, operation can be selected to provide the input signals either internally or from externally connected devices.

The Newera Trainer Kit [10] runs on an open source real-time Linux operating system. A SCADA program is ran on a separate PC and is not part of the kit. The kit incorporates all control functionality in software modules so no PLCs or other electronics are required for control. A simulator box allows analog and digital signals to be interfaced with the controller software. This kit is advertised as a possible SCADA trainer but seems to be a simulated control system (PLC simulation). While this system can interface with SCADA software, the user is free to choose the SCADA package of his/her choice.

E-Learning Online SCADA Training [11] is a series of compact discs with curricula and SCADA software included. This training package advertises that the user can use the supplied SCADA software to create screens and objects and then test the design through simulation. No additional details were given other than the $100 cost for each compact disc. Interactive Graphical SCADA System [12] software by 7-Technologies is a full featured software package that allows for SCADA project development with no extra modules or add-ons required. The software is hardware independent utilizing communications drivers that are optimized for Interactive Graphical SCADA System (IGSS) but also support OPC. A controller system of the user's choice would need to be added to develop an operational trainer.

3. TOOLKIT DESCRIPTION

Two portable SCADA security toolkits are currently being developed and are described in detail in the following sub-sections.

3.1 Toolkit I

The first toolkit, shown in Figure 1, consists of a power supply, a controller, and a router mounted inside a plastic carrying case. It also has two push buttons (red and green), two lamp lights (red and green), and a 1KΩ potentiometer mounted on the top of the case's lid.

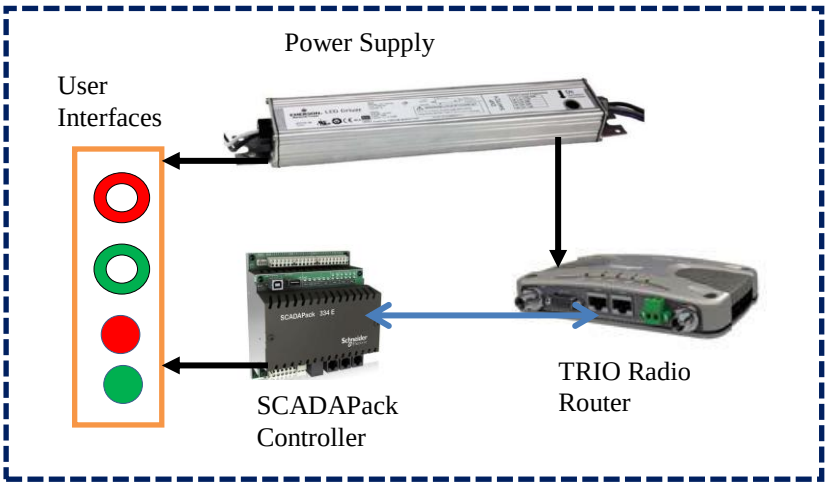

Figure 1. Toolkit I

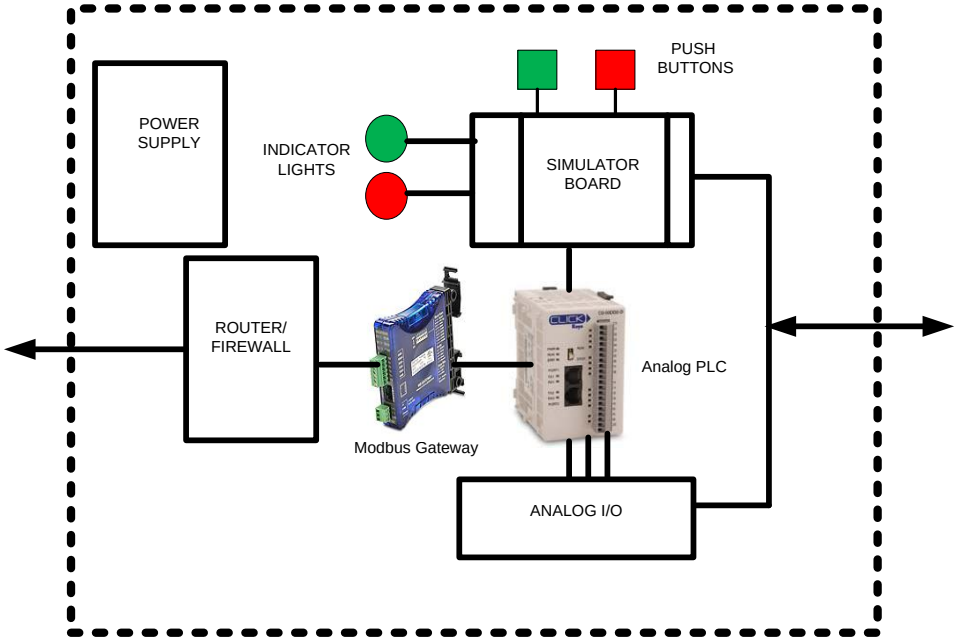

Figure 2. Toolkit II

The power supply, a Mean Well CEN 75-30, can have its voltage output adjusted between 26-30 volts and its direct current output adjusted between 1.88-2.5 amperes. It provides power to all of the other components. The controller is a SCADAPack 334 E made by Control Microsystems, a subsidiary of Schneider Electric. It is an RTU with 16 digital inputs, 8 analog inputs, and 10 relay outputs. It has a 32-bit microcontroller with a 32 MHz clock, 16MB of Flash ROM, 4MB of CMOS RAM, and 4kB of EEPROM. Its communication capabilities include a high speed Ethernet connection, as well as RS-232, RS-485, and USB connectors. The controller supports standard industry Modbus, serial DNP3, and Modbus TCP and UDP-based Ethernet protocols. The router, a Trio Radio (JR900) that is also made by Control Microsystems, allows for wireless data transfer between remote field devices and the controller using either the 900MHz or 2.4GHz frequency band. The radio is equipped with antennas that can receive data from remote devices. The data are then relayed to the controller through a cable.

3.2 Toolkit II

The block diagram of the second toolkit is shown in Figure 2. It consists of a PLC (Automation Direct Micro Analog PLC), a Virtual Private Network (VPN) router/firewall (TrendNet TW100-BRV204), a Modbus Gateway, an analog I/O module (F0-08ADH-1-8), a power supply, two push buttons (green and red) and two pilot lights (green and red). Both kits are designed to address critical issues on control engineering and network security. Each kit will also include the following software components: a PLC/RTU programming software, an HMI, and a customized user interface for controlling the PLC/RTU and emulating its input and output. The PLC/RTU included in the toolkits is used to implement some control actions such as turning ON/OFF the pilot lights by either pressing the push buttons or using the HMI. Basic network security functions are implemented using the VPN router/firewall, which is used to interface with the external network. The PLC should be equipped with at least two communication ports in order to exchange information with both the router and the PC.

4. TOOLKIT LEARNING ACTIVITIES MODULES

The initial curriculum modules that we designed and implemented to accompany these toolkits are outlined in the following:

Module Name: Computer Networks
Learning Objectives: To understand basic computer networking concepts and communication protocols
Prerequisite: Basic knowledge of computer systems
Topic Outline:
- The network layer standards: OSI vs TCP/IP
- Basic routing and addressing
- Network and port address translation
- Switches and routers
- Virtual Private Networks (VPNs) and Virtual Local Area Networks (VLANs)

Associated Practical Laboratory Exercises:
- Setting-up a Local Area Network
- Configuring the toolkit for Internet access

Module Name: Computer Security
Learning Objectives: To understand basic computer security concepts and associated practices
Prerequisite: Basic knowledge of computer systems and networking fundamentals
Topic Outline:
- Basic computer security concepts
- Access Control, Authentication, and Authorization

Associated Practical Laboratory Exercises:
- Scanning and mapping a target network
- Packet sniffing and analysis
- Configuring the toolkit for VPN connection

Module Name: Firewall Configuration
Learning Objectives: To understand basic firewall configuration to enable basic authorization and accounting
Prerequisite: Basic knowledge of computer networks, routing protocols, and security principles
Topic Outline:
- Understanding basic firewall rule configuration
- Configure Authentication, Authorization, and Accounting (AAA)
- Configure a modular policy framework

Associated Practical Laboratory Exercises:
- Configure and test a firewall configuration
- Design and implement a secure firewall configuration for the toolkit

Module Name: PLC Programming and Toolkit Customization
Learning Objectives: To understand the basic functions and programming of PLCs/ toolkit PLC programming
Prerequisite: Basic knowledge of control devices and associated protocols.
Topic Outline:
- PLC programming
- Visual Basic programming

Associated Practical Laboratory Exercises:
- PLC programming

- Creating a control system Human Machine Interface (HMI)
- Customizing the toolkit

5. TOOLKIT LEARNING PROJECTS

The following describes the pedagogical projects associated with these toolkits. These hands-on learning activities were developed and implemented to reinforce the concepts of wireless communication, information security, control protocols such as Modbus/TCP and DNP3, HMI design and implementation, automation programming, and circuit design.

a. HMI Design and Implementation Project

Objective: Design an HMI for a water pumping station that will simulate two water pumps (supply and discharge) connected to a tank tower and controlled by a SCADAPack controller running the Modbus/TCP protocol. Prerequisite Knowledge: Visual Studio development environment and Modbus TCP protocol. Deliverables: Functional HMI that controls a PLC running on Modbus/TCP. A sample deliverable is shown in Figure 3.

b. IEC61131-3 Programming

Objective: Write an automation program that implements the following specification on a SCADAPack controller. This program will simulate the operation of a waste water pump system. A built-in potentiometer will simulate the varying water level in a water tank. Thus, the potentiometer's varying resistance raises and lowers the current input to the RTU controller, which in turn simulates the water level in a tank. Once this level reaches an upper threshold, a red lamp light becomes energized and blinks every two seconds, warning that the water level is too high. At the same time a green lamp light becomes energized indicating that a pump has turned "On" to discharge the excess water out of the system. When the potentiometer adjusts the water level to a lower threshold, the outputs turn "Off". The push buttons simulate manual overrides for the pump in the system. A green push button manually turns the pump and green lamp light "On" and a red push button turns those outputs "Off".

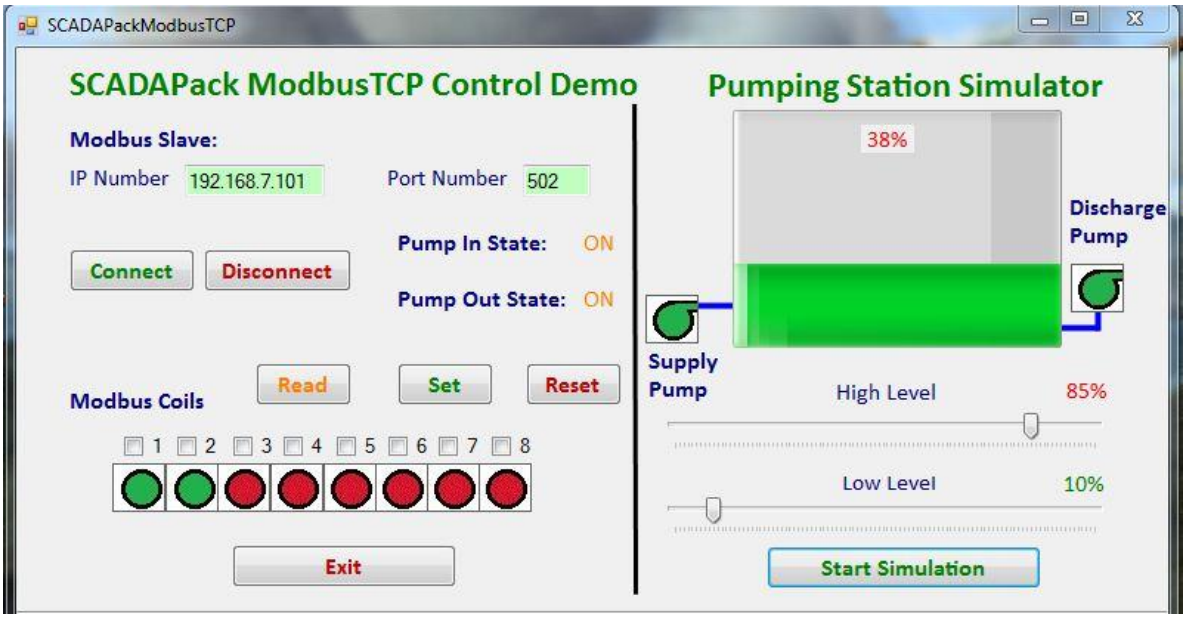

Figure 3. HMI for Simulator

The International Electro-technical Commission (IEC) [14] has published the IEC61131-3 standard for automation programming languages. This standard is implemented by the ISaGRAF 3.55 [15] workbench and programming suite, which offers all five of the languages defined in the standard: ladder diagram, function block diagram, instruction list, structured text, and sequential function chart. Prerequisite Knowledge: Automation programming. Prior knowledge on the ISaGRAF workbench is optional. Deliverables: Automation program implemented and downloaded to the SCADAPack controller.

A sample deliverable program is shown on Figure 4. This program is primarily composed of the function block diagram and ladder diagram languages. The *Analog_In* is where the direct current is coming

in from the potentiometer. The *Scaling block* that is tied to it will take the level of current and convert it to a number of increments ranging from 0-10000. It is then able to convert those increments into a percentage that is displayed in the *Tank_level* block [16]. The upper (*Upper_Thr*) and lower (*Lower_Thr*) inputs connected to the <= and >= blocks contain constant values that represent the lower and upper threshold levels in the tank. The <= and >= blocks compare these thresholds with the inputs coming from the Scaling block and determine if the comparison is *true* or *false.* In this example, if the water level reaches at or above the 75% threshold mark, the >= block will become *true* and energize the *set* coil (S) with the name *set_2.* This means that the contact above with the name *set_2* will close, providing a path for current to turn on the red pilot light (RPL), pump, and green pilot light (GPL). The *reset* coil (R), connected to the <= block, will turn the set coil *Off* when the water level reaches at or below the 50% threshold mark. This will also turn *Off* the RPL, pump, and GPL.

Notice that the RPL is connected to a *blink* function block. This is what makes the RPL blink every two seconds, simulating a warning light. Set and re-set coils are also used for the upper part of the program as well. The set coil in the top rung "locks" in the GPL and pump once the green pushbutton (GPB) is pressed. When the red pushbutton (RPB) is pressed, a re-set coil is then energized and stops the set coil, which also stops the pump and GPL. These coils are only logical, and do not actually have any direct association with the outputs of the RTU. Any contact with the same name as a coil will respond according to the state (true/false) of the coil.

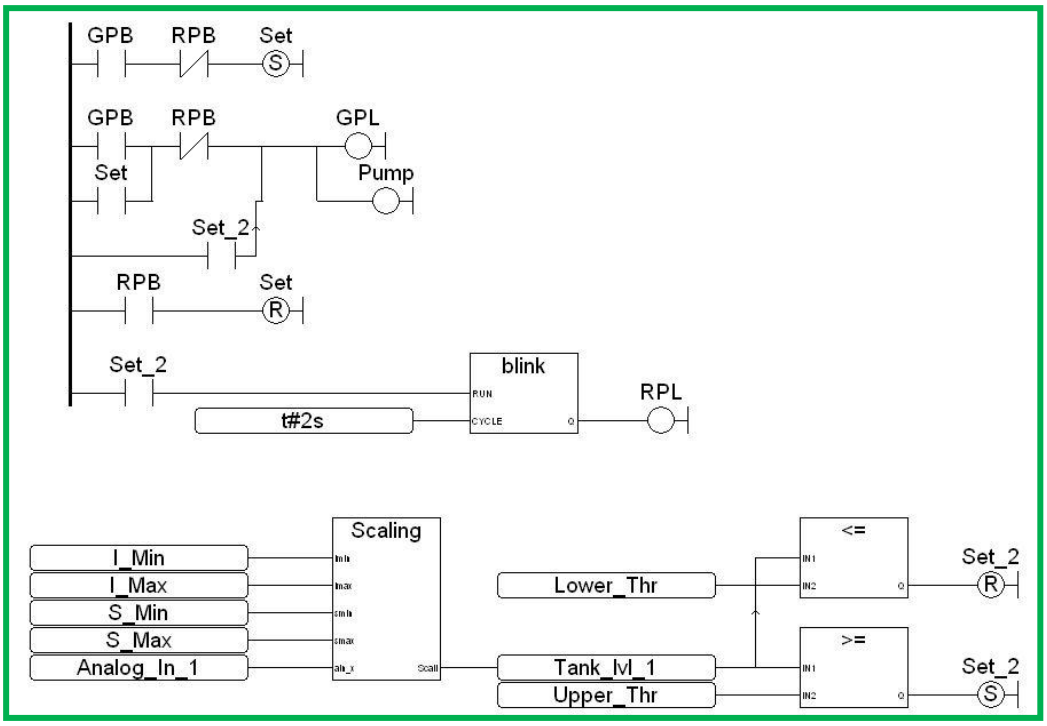

Figure 4. Control Program

c. Wireless Connectivity Project

Objective: Configure two 900-MHz Trio Radios to function as an Access Point and as a wireless bridge respectively. Prerequisite Knowledge: Configuring wireless devices, TCP/IP protocol, network subnetting. Deliverables: Fully connected wireless network of SCADAPack controllers.

d. Vulnerability Analysis of SCADA Networks

Objective: Perform a vulnerability analysis of wireless SCADA networks which are configured for the 802.11 protocol and the 900-MHz radio. Prerequisite Knowledge: Familiarity with a network mapping tool such as nmap, a network sniffing tool such as wireshark, a password cracking tool such as hydra, and a packet builder tool such as Colasoft. Deliverables: Vulnerability analysis report of the SCADA toolkit network.

e. Calculating Voltage Drop Resistors

Objective: Calculate the resistance and wattage values of a voltage drop resistor in order to allow a 5 volt (V) direct current (DC) to pass from a power supply source to its series-connected load (e.g. a lamp or an LED). Prerequisite Knowledge: Basic knowledge of DC circuits. Deliverables: Cost effective way to connect loads requiring different voltages to a single power supply source. Unlike many PLC controllers, the digital outputs of the SCADA Pack RTUs-such as the one used in the 1st toolkit mentioned above-do not actually output any voltage. This means that the power supply voltage may have to be stepped down in order to provide the necessary voltage for light indicators, small motors, etc. that are connected to the RTU. Since the wrong voltage can potentially damage the RTU and/or the load, using voltage drop resistors are a safe and a cost effective way to accomplish this task. In this scenario, a 30V, DC power supply needs to have its voltage lowered in order to power a 5 V, 90 milli-ampere (mA) light bulb indicator. It is decided that a series resistor will be used to accomplish this task. The following steps are used for determining the resistance and wattage values that are needed:

1. Determine the maximum load current (I_L): the maximum current used by the light bulb is listed on its specification sheet to be 90mA.
2. Calculate the resistance for the voltage drop resistor (R_D): the voltage to be dropped across R_D (V_R) is approximately 25 V since the bulb is rated at 5V and the source voltage is 30V, thus 30V-5V=25V. Therefore, by using Ohm's Law, $R_D = V_R/I_L = \frac{25v}{90mA} = 277.78\Omega$. Rounding up to the nearest standard resistor value, a 300 ohm resistor is needed.
3. Calculate the power dissipation or wattage (W) of R_D, then add 25% for safety: using $V_R * I_L * 1.25$, $25V * 90\ mA * 1.25 = 2.8W$, which is then rounded up to 3W for added safety.

The above example is only a hypothetical scenario and is not intended to represent the only factors to be considered when determining a proper sized resistor. If the resistor is exposed to potential human contact, its amount of heat dissipation may be a safety concern. Therefore it may be wise to inquire about the resistor's temperature at its calculated wattage value. This may lead to choosing a higher wattage value that will be deemed safer.

6. CONCLUSIONS AND FUTURE PLANS

Cybersecurity and cyberwarefare are among two of the most important buzzwords that are currently prevalent in the media. The national government recognizes the need to address these critical issues. After all, in this modern age our very lifestyles and well-being are dependent upon the preservation and sustenance of cyberspace. One of the most effective ways to meet the challenges presented by these issues is through education and training. This project is an instrument to that purpose. Our modest contribution is the development and dissemination of curriculum materials and pedagogical implements that enhances cybersecurity education and training. This paper presented a review of SCADA system learning toolkits and described our own cost-effective way of equipping educators with hands-on toolkits that they can deploy in their classrooms and use as security testing and learning kits. We also outlined several control system security curriculum modules that can be adopted and deployed in K-12 and higher education institutions. The challenge for the authors will be to further develop these toolkits and to enhance the learning modules used with them. Furthermore, the design and implementation of virtual learning simulators, which will provide online cybersecurity laboratory exercises, are also on the horizon. These simulators will be freely shared through the Internet and will provide a cost-effective way of providing a broader and lasting impact to the realm of control system security education.

7. ACKNOWLEDGEMENTS

This paper is based upon a project partly supported by the National Science Foundation under grant awards OCI-0959687 and DUE-0726486. Opinions expressed are those of the authors and not necessarily of the Foundation.

REFERENCES

[1] Association for Computing Machinery (ACM)/IEEE Computer Society Interim Review Task Force, "Computer Science Curriculum 2008: An Interim Revision of CS 2001," URL: http://www.acm.org//education/curricula/ComputerScience2008.pdf. December, 2008.
[2] P. Auerswald, L.M. Branscomb, S. Shirk, M. Kleeman, T.M. Porte, and R. N. Ellis, "Critical Infrastructure and Control Systems Security Curriculum," *Department of Homeland Security, version 1.0*, Washington, DC, March, 2008.
[3] G. A. Francia III, "Critical Infrastructure Curriculum Modules," *Proceedings of the 2011 Information Security Curriculum Development Conference. Kennesaw, GA. October 2011*.

[4] J. Pollet, "Developing a Solid SCADA Security Strategy," *2nd ISA/IEEE Sensors for Industry Conference, pp.148-156, Nov. 19-21, 2002*.
[5] President's Commission on Critical Infrastructure Protection, "Critical Foundations-Protecting America's Infrastructures." Website: http://www.fas.org/sgp/library/pccip.pdf.
[6] President's Critical Infrastructure Protection Board and the Department of Energy, "21 Steps to Improve Cyber Security of SCADA Networks." URL: http://www.oe.netl.doe.gov/docs/prepare/21stepsbooklet.pdf.
[7] United States Government Accountability Office (GAO), "Critical Infrastructure Protection DHS Needs to Fully Address Lessons Learned from Its First Cyber Storm Exercise." *Report GAO-08-825, September 2008*.
[8] CYBATI. Website: https://cybati.org/business/hands-on-onsite-control-system-cyber-security-course. Last access: February 28, 2012.
[9] Interlabs, "Programmable Logic Control Trainer Model IBL-29." Website: http://www.interlabs-india.com/process-control-instruments.html. Last access; March 01, 2012.
[10] Newera Controls, "Newera GCS Trainer Kit." Website:http://www.neweracontrols.com/index.php/partner-with-newera-controls/newera-gcs-trainer-kit. Last access: March 02, 2012.
[11] ScanTime, "E-Learning Online SCADA." Website: http://www.scantime.co.uk/html/plc_learn_online_scda12.htm. Last access: March 02, 2012.
[12] 7-Technologies, "Interactive Graphical SCADA System (IGSS)." Website: http://www.igss.com/index.htm. Last access: March 02, 2012.
[13] Byres Security, Inc. "Tofino SCADA Security Simulator," Website: http://www.tofinosecurity.com/products/tofino-scada-security-simulator. Last access: March 05, 2012.
[14] International Electrotechnical Commission (IEC). Website: http://www.iec.ch. Last access: March 08, 2012.
[15] ISaGRAF Workbench. Website: http://www.isagraf.com. Last access: March 02, 2012.
[16] Control Microsystems Inc, "IEC 61131-3 Product Training: Telemetry & Remote SCADA Solutions" *Manual 2006*.
[17] DNP Users Group (2012), "Overview of the DNP3 Protocol." Website: http://www.dnp.org/Pages/AboutDefault.aspx. Last access: May 22, 2012.
[18] Triangle MicroWorks, Inc. (2012), "DNP3 Overview." Website: http://www.trianglemicroworks.com/documents/DNP3_Overview.pdf. Last access: May 22, 2012.
[19] G. Clarke, D. Reynders, and E. Wright, "Practical Modern SCADA Protocols: DNP3, 60870.5 and Related Systems." *IDC Technologies, Elsevier Ltd. 2004*.
[20] Real Time Automation. "DeviceNet Introduction." Website: http://www.rtaautomation.com/devicenet/. Last access: May 22, 2012.
[21] Rockwell Automation. "Ethernet/IP Network Overview." Website: http://www.ab.com/en/epub/catalogs/12762/2181376/214372/1810894/3404056/Introduction.html. Last access: May 22, 2012.
[22] Open DeviceNet Vendors Association (ODVA). "DeviceNet Technology Overview." Website: http://www.odva.org/Home/ODVATECHNOLOGIES/DeviceNet/DeviceNetTechnologyOverview/tabid/72/lng/en-US/Default.aspx. Last access: May 22, 2012.
[23] Open DeviceNet Vendors Association (ODVA). "Common Industrial Protocol (CIP)." Website: http://www.odva.org/Portals/0/library/publications_numbered/PUB00122R0_CIP_Brochure_ENGLISH.pdf. Last access: May 22, 2012.

BIOGRAPHY OF AUTHORS

Dr. Guillermo A. Francia, III received his BS in Mechanical Engineering degree from Mapua Tech in 1978. His Ph.D. in Computer Science is from New Mexico Tech. Before joining Jacksonville State University (JSU), he was the chairman of the Computer Science department at Kansas Wesleyan University. Dr. Francia is a recipient of numerous grants. His projects have been funded by prestigious institutions such as the National Science Foundation, Eisenhower Foundation, Department of Education, Department of Defense, and Microsoft Corporation. Dr. Francia served as a Fulbright scholar to Malta in 2007. He has published articles and book chapters on numerous subjects such as Computer Security, Digital Forensics, Regulatory Compliance, Educational Technology, Expert Systems, Computer Networking, Software Testing, and Parallel Processing. Currently, Dr. Francia is the Director of the Center for Information Security and Assurance at JSU.

Dr. Noureddine Bekhouche received his BS in Electrical Engineering from the University of Annaba. He received his Ph.D. in Electrical Engineering from West Virginia University. He teaches AC/DC Circuits; Electronic Devices; Advanced Electronics; Electronic Microprocessors; Programmable Controllers; Control Systems; Robotics; and Applied Digital Communications Systems. His area of interest is Control Systems and its applications. In particular, he has experience in electric utilities operation and generation control. He is currently a Professor of Engineering and Technology at JSU.

Mr. Terry Marbut received his BS and MS in Electrical Engineering at the University of Alabama in Birmingham. He teaches Microcomputers: Applications and Techniques; AC/DC Circuits; Electronic Devices; Advanced Electronics; Electronic Microprocessors and Communications; and Applied Digital Communications Systems. Currently, he is the head of the Technology and Engineering Department at JSU.

Curtis Neuman, an honor student at Jacksonville State University, will soon graduate with a B.S. in Applied Electronics Engineering at JSU. He is responsible for the mounting design, construction, and programming of Toolkit I.