SCADA Security

Devin Raposo

Final Submission

April 3rd, 2018

CEN 3078 Software Security

Instructor: Dr. Janusz Zalewski

Department of Software Engineering

Florida Gulf Coast University

Ft. Myers, FL 33965

1. Introduction

Within the broad landscape of software security, there exist many forms of software which function as control system architectures [1] for large industry applications. One such control system architecture is known as Supervisory Control and Data Acquisition, abbreviated as SCADA. SCADA systems “are at the heart of the modern industrial enterprise ranging from mining plants, water and electrical utility installations to oil and gas plants.” [2] In other words, SCADA systems act autonomously to ensure the proper, secure, and safe functionality of a large variety of automated systems, infrastructure, and machinery which make up the bulk of productivity apparatuses within industries. More specifically, SCADA systems, “maintain efficiency, process smarter decisions, and communicate system issues to help mitigate downtime.” [3] At the base level of SCADA architecture exists programmable logic controllers (PLC) [4] as well as remote terminal units (RTU) [5], which are microcomputers which communicate with hardware objects like factory machines, human machine interfaces (HMI) [6] used by humans to interface with the SCADA devices, sensors, and end devices. They then are able to route these information from the physical objects to computers via proprietary SCADA software. These software are able to process, distribute, and display these data, which can help system operators and other employees to analyze these data and make critical decisions. [3] These data are able to be communicated from the PLC’s and RTU’s to the SCADA software via Local Area Network (LAN) [7] and Wide Area Network (WAN) [8] connections. For example, in the event of some form of error in hardware functionality, the SCADA system can automatically detect the issue and alert an operator’s HMI device via the network connection so that the operator will be made aware of the issue and can make a corresponding decision on how best to mitigate the issue. Additionally, the processes being performed by the infrastructure being overseen by the SCADA control architecture can be monitored remotely by the human operator as it proceeds via the HMI. SCADA’s automated and remote connectivity properties make it a useful and efficient means to monitor the scenarios of industry. A broad overview of this monitoring control loop is provided visually in Figure 1, which was created by Inductive Automation for their article on SCADA [3]. For its simplicity, stability, and versatility within a variety of leading industry productivity pipelines, SCADA has become the de facto solution to automated hardware and software processes which together contribute to industrial growth.

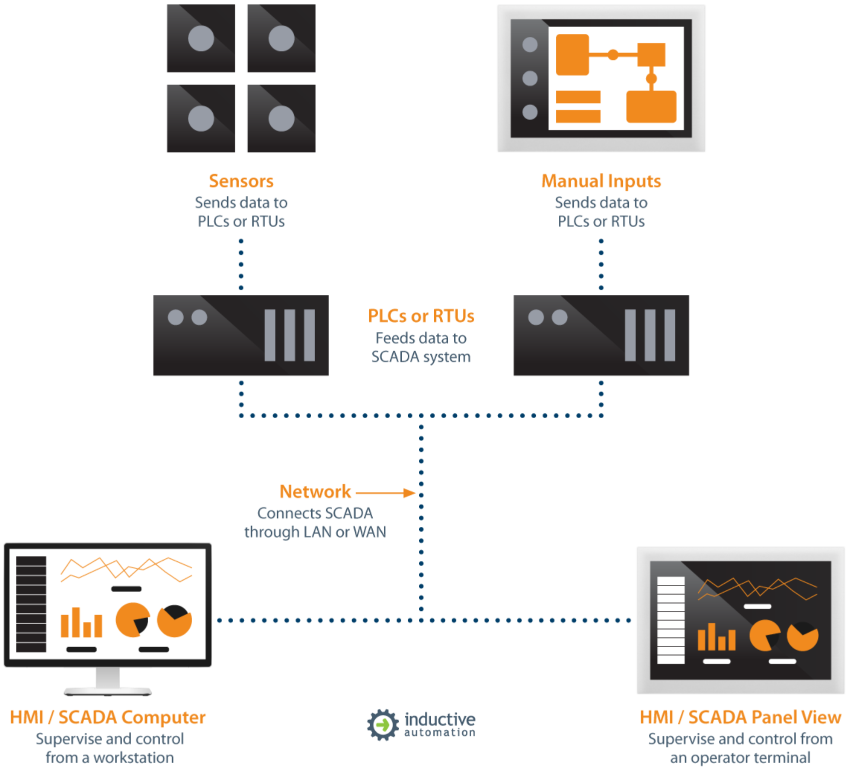

Sensors
Sends data to PLCs or RTUs
Manual Inputs
Sends data to PLCs or RTUs
PLCs or RTUs
Feeds data to SCADA system
Network
Connects SCADA through LAN or WAN
HMI / SCADA Computer
Supervise and control from a workstation
inductive automation
HMI / SCADA Panel View
Supervise and control from an operator terminal

Figure 1. SCADA Architectural Infrastructure [3]

2. Principles of the Technology

To describe the core principles of the SCADA automation architecture, it is necessary to undergo a description of each of the core SCADA system constituent components, as well as how they interact together to form an architecture capable of monitoring enterprise-grade industry operations.

2.1 Programmable Logic Controllers

Programmable Logic Controllers (PLC) are the core of the SCADA infrastructure. Figure 2 displays a general schematic of a Programmable Logic Controller.

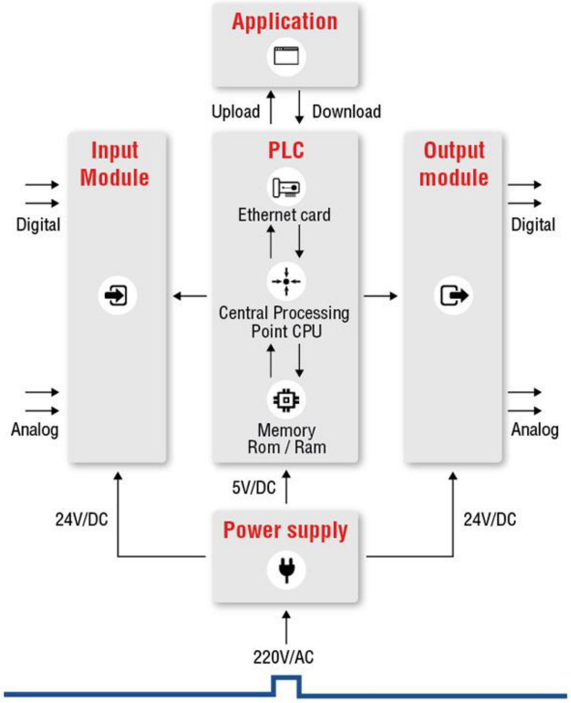


Figure 2. Programmable Logic Controller Diagram [9]

PLC’s are responsible for receiving local data inputs and transmitting these data as outputs via a physical networked connection over Ethernet to an HMI for a human operator to visibly see and respond to, or to other machinery within the control loop architecture. The PLC’s CPU stores and processes program data, and then input/output (I/O) modules provide information to the CPU so as to trigger specific results. [9] Inputs may come from the area that the PLC is situated in by a sensor or other machines which exist in the control loop, or they may arrive via a network connection from the human operator using the HMI. These data received by the PLC may arrive from thousands of sensors which exist in the environment the PLC is placed in, as is often necessary in large industrial environments. These data may also arrive from other Remote Terminal Units (RTU), devices which are capable of interfacing with physical non-software apparatuses which exist in the workflow environment. Section 2.2 is concerned with RTU's. Figure 3 demonstrates a connection between a personal computer (PC) acting as an HMI to interface with a variety of PLC's and Distributed Control Systems (DCS), each of which are connected to the sensors for data input.

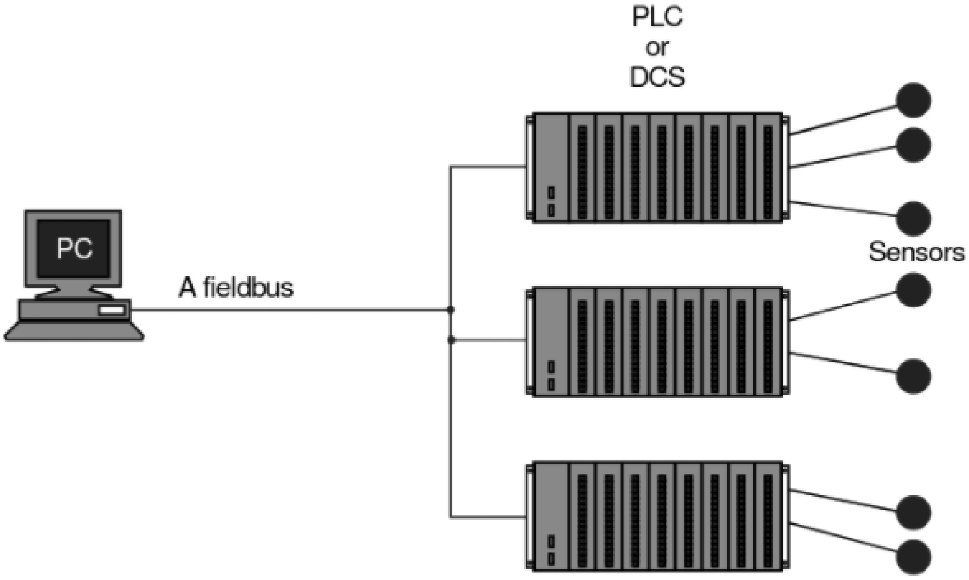


Figure 3. HMI to PLC/DCS connection interface [10]

As requirements for systems grew, the development of these sensors evolved and erased the need for PLC's to be in place. [10] They became known as Intelligent Electronic Devices (IED) [11] and are connected on a fieldbus [12] to the HMI. Figure 4 shows an illustration of a PC acting as HMI connecting directly to a series of IED's via a fieldbus connection.

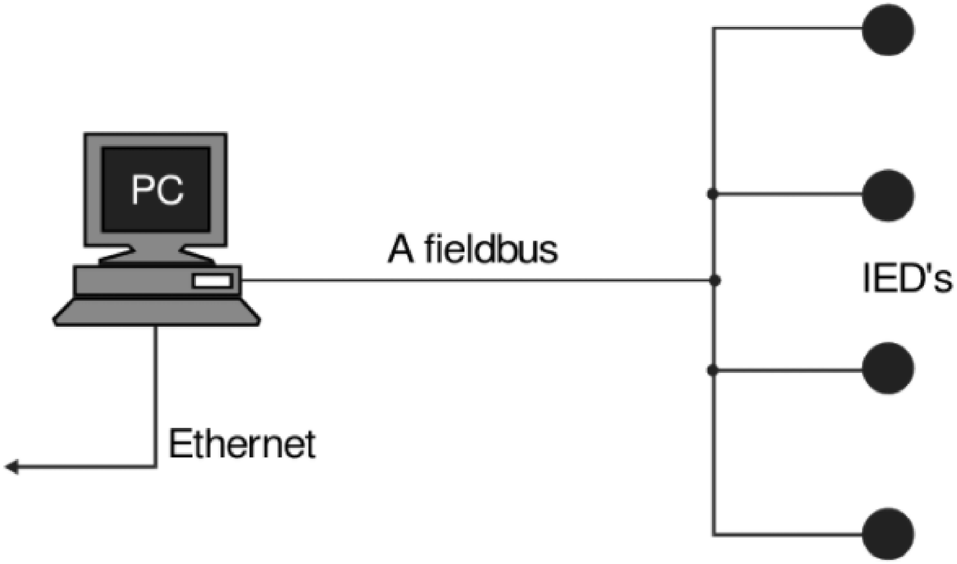


Figure 4. HMI to IED connection interface [10]

Figure 5 shows a picture taken of an actual PLC.

Figure 5. Programmable Logic Controller [13]

2.2 Remote Terminal Unit

Remote Terminal Units (RTU) are devices which primarily are concerned with the retrieval of data from which exist in the industrial work environment. In more general terms, their core purpose is to retrieve field data and transmit these data wirelessly to some outside entity to make decisions about that data, whether that be a machine or an HMI for a human to interface with. [10] RTU's essentially provide the HMI with a remote interface to the field analog and digital sensors which exist onsite. In fact, the HMI is in itself an RTU. RTU's, unlike PLC's, use wireless communication, and thus are more suitable for applications over large geographical areas. They connect wirelessly to remote central SCADA monitoring systems. Unlike PLC's, RTU's generally speaking are not concerned with actual local control of devices. Instead, they are merely concerned with the transmission of data the RTU receives from local sensors to a master control station which will then decide whether to query the PLC's of a worksite to perform some action on other devices. RTU's, then, are useful for diagnostics of onsite devices to HMI's and other control systems. Figure 6 demonstrates an abstraction of a connection between several onsite RTU's to a SCADA database control system via a network connection.

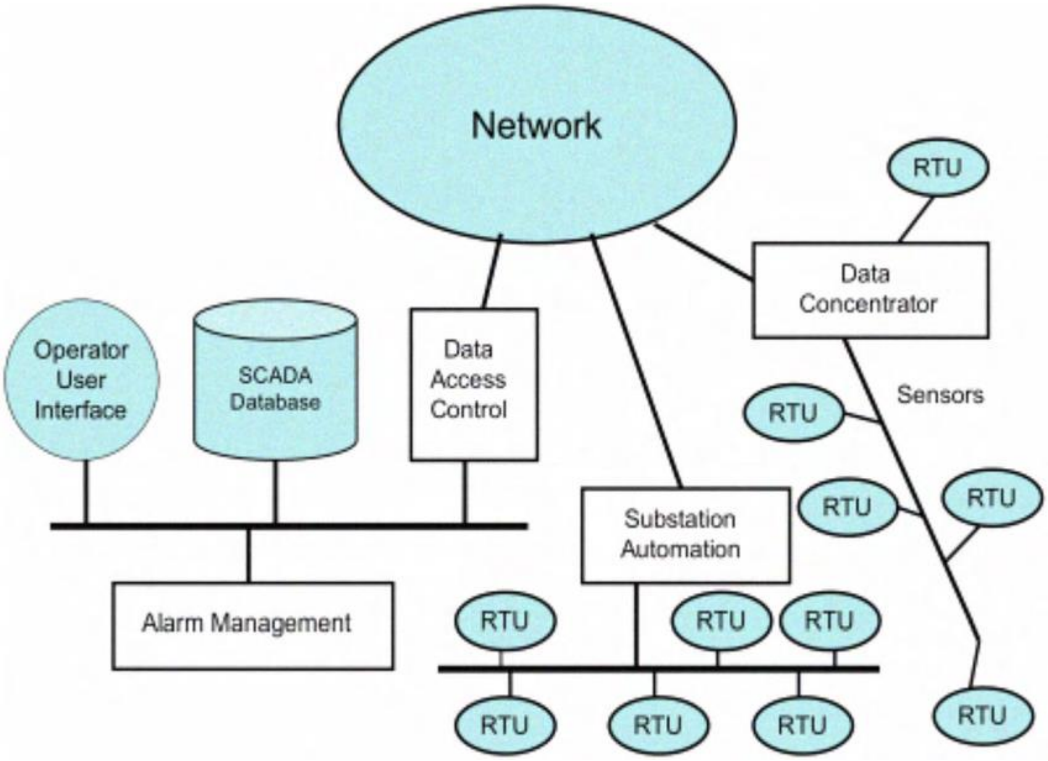


Figure 6. RTU to SCADA Database Control System Connection [14]

Figure 7 shows a picture of an actual onsite RTU.

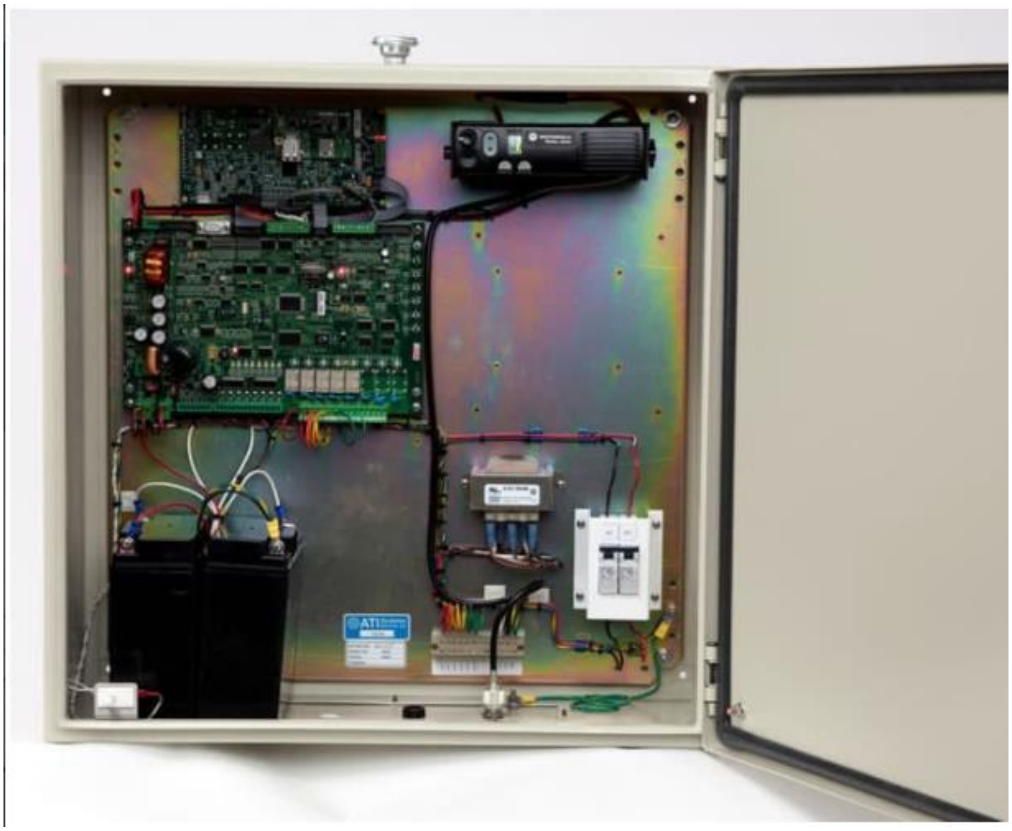


Figure 7. Onsite Remote Terminal Unit [15]

2.3 SCADA Software

It is necessary for SCADA systems to include software interfaces which can act autonomously as well as interface with humans via the usage of HMI's. These can be either proprietary – developed internally by companies as their own - or open, solutions purchased and licensed by other companies for use. A popular example of an open SCADA software solution is Wonderware [16]. SCADA software solutions visualize those data received via RTU's and PLC's over wireless and local network connections, respectively, and thus serve as the diagnostics apparatus by which a human operator can develop an understanding of operational going-ons at the worksite. These data can then be used to make on-the-fly decisions, whether by a human operator or autonomously via a SCADA software which serves as a master control system. A SCADA software solution will offer functionality for operators to assign PLC's to have a device do, such as changing the temperature of an apparatus or changing the rate at which a process occurs. SCADA software solutions can be set to perform such functions autonomously, eliminating the need for human operators to perform all of them and freeing up bandwidth for other tasks. These software exist on PC's which connect to remote PLC's and RTU's via local or wireless network connections, more specifically via radio, fiber optic and infrared systems. [10] Figure 8 demonstrates a typical SCADA system where the SCADA software solutions runs on the Display Servers.

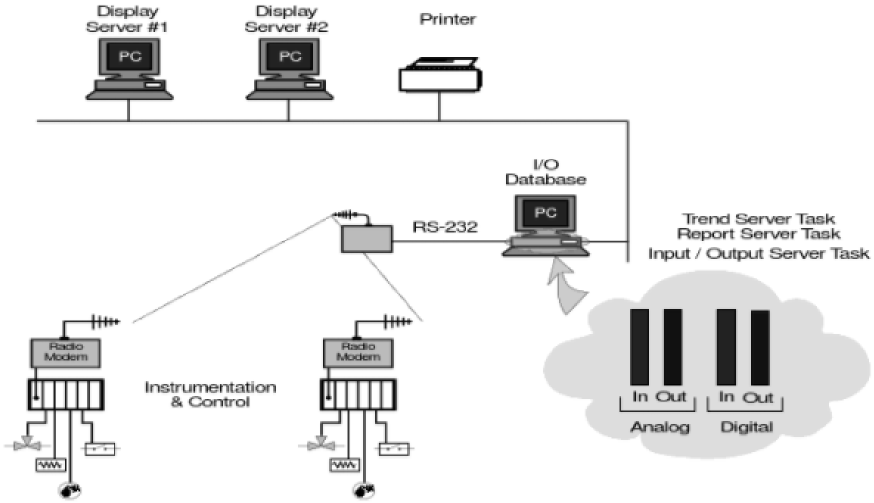


Figure 8. SCADA System with Software Solution [10]

Figure 9 shows an example of a visual user interface for Wonderware, the aforementioned SCALA software solution.

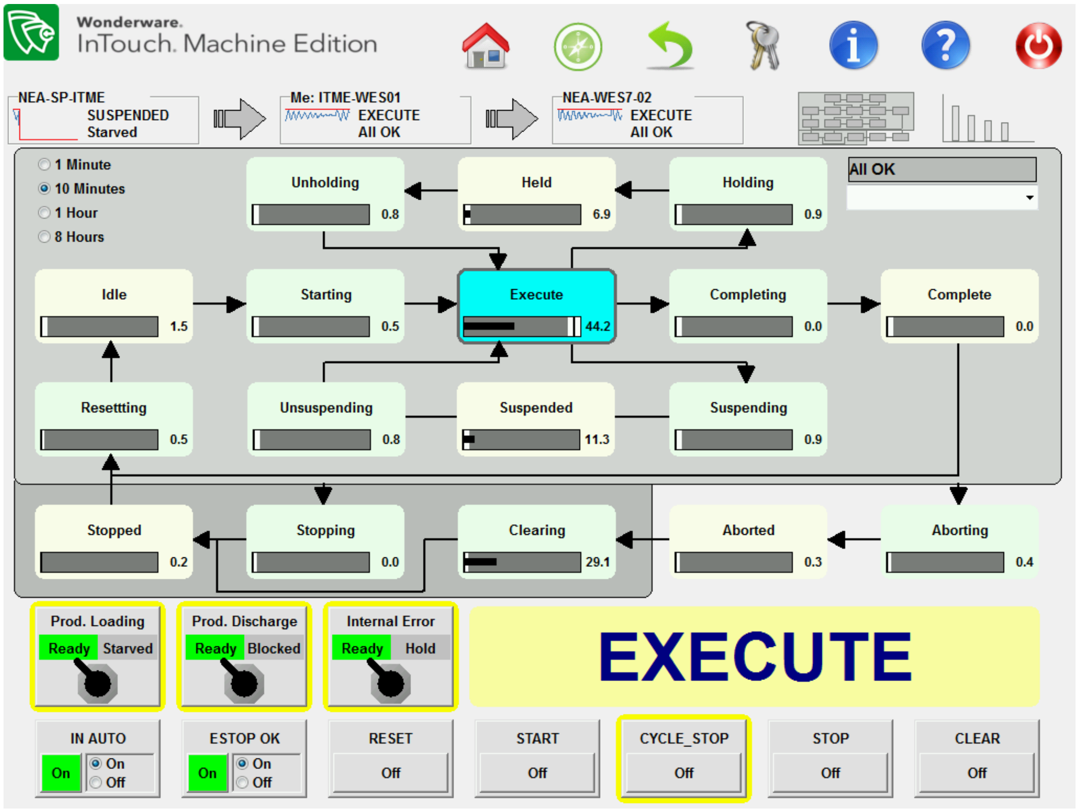


Figure 9. Wonderware Visual User Interface [16]

3. Securing the Technology

It is important now to discuss in specific terms the ways in which the SCADA technology is secured from outside threats and vulnerabilities. In order to discuss these methodologies, it is first necessary to identify these vulnerabilities and threats. Section 3.1 introduces the source of these vulnerabilities and threats. Section 3.2 proceeds to take a close examination at the various technologies and methodologies used to secure SCADA in light of these vulnerabilities and threats.

3.1 Vulnerabilities and Threats

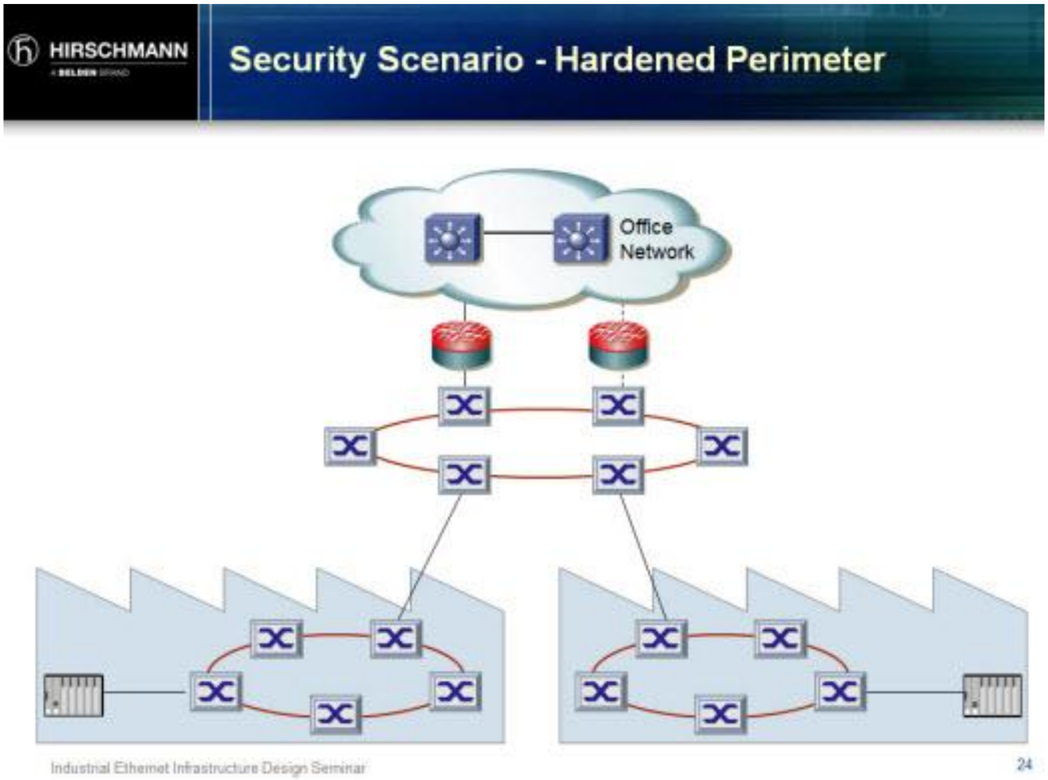
At the dawn of the introduction of PLC's and RTU's, generally speaking there was far less of a concept of 'cybersecurity'. [18] As PLC's and RTU's are both enormous factors within the general architecture of SCADA, one can imagine how this might affect industry ability to best secure the technology later down the line. Of course, today there are PLC's and RTU's which are designed with a further awareness and mindfulness for security against threats, but it is a reality that many industry applications of PLC's and RTU's shall still incorporate older and more out-of-date technologies for reasons of cost. Even newer models of PLC's and RTU's may be made outdated within a short period of time following their installation in an industrial environment. These—in addition to older models, of course—can be designated as vulnerable when they run for weeks or months without obtaining a security update. Some devices might be lacking in proper anti-virus software which could help to identify and eliminate software threats made by any outside entities with intent of malice. Malformed and evenly correctly-formed traffic too can be an issue for certain PLC's [19].

There exist multiple pathways upon which malware can enter a SCADA system, not just remotely via a network connection. Physical laptops as well as USB drives [20] can also be used to bypass any network connections so as to introduce a threat to a closed industry SCADA system. Malware such as this could in turn be introduced to other systems within the industrial environment. [19] This problem can further be exacerbated by older "flat" networks, which are networks that are not isolated from each other and instead constitute a single conglomerate network, thus making the spread of illicit malwares which create threats and exploit vulnerabilities far quicker and more efficient from the perspective of the perpetrator. [19]

More broadly speaking, threats to the security of SCADA systems have only been further exacerbated over time as the world becomes more and more interconnected at a network level. SCADA systems are also extremely reliant on performance; any semblance of latency introduced to a SCADA system can be detrimental to its ability to perform its core tasks. So, for example, performing a port scan could unintentionally open the system to vulnerabilities. [19]

3.2 Securing SCADA

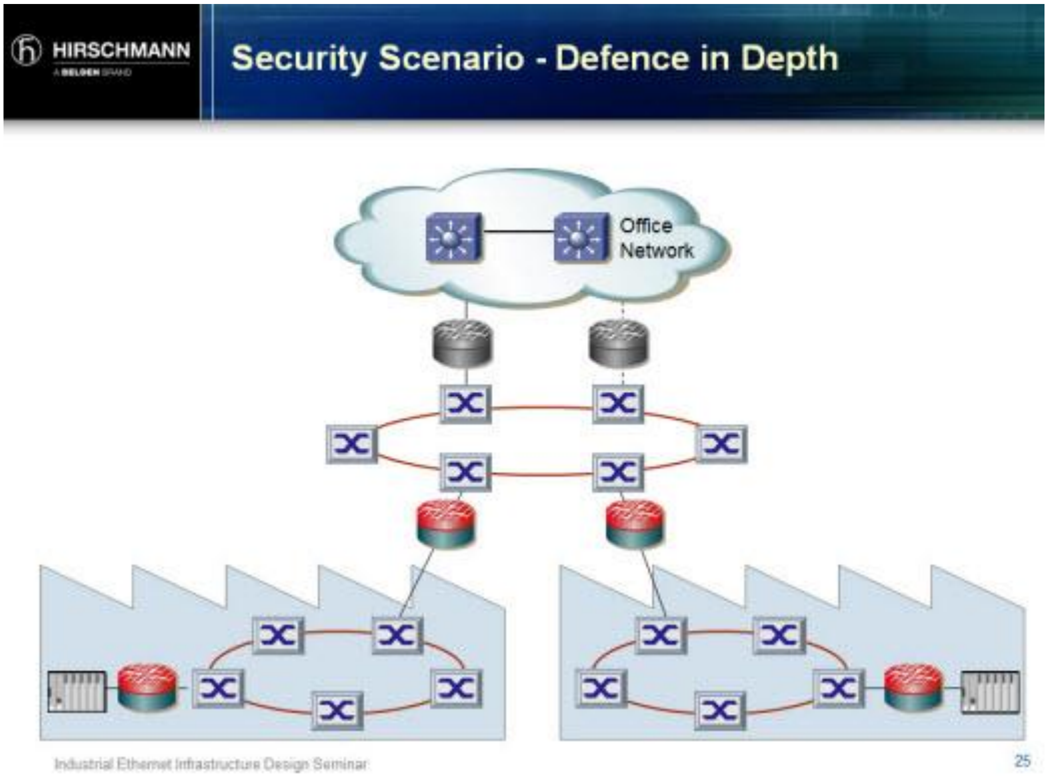
In general, the security dimensions which are most important for a SCADA system to focus on protecting are integrity and availability; confidentiality matters much less here. [21] The first and most obvious way to introduce cybersecurity to SCADA systems in a way which mitigates many of the issues addressed in Section 3.1 is harden perimeters between devices and networks. In other words, increase the level of separation of systems, compartmentalizing them and making them less modular. This way, if an issue is introduced in one network/device, it won’t have farther-reaching implications for other networks/devices within the same SCADA system. [19] Figure 10 below displays a visual representation of this concept of “hardening the perimeter.”



Security Scenario - Hardened Perimeter

Figure 10. Hardening the Perimeter of a SCADA System [19]

There exists a concept in computing known as ‘Defense in Depth’ which states that it is better to have multiple layers of defense as opposed to a single barricade blocking entryway. In this particular scenario regarding security in SCADA networks, the concept can be applied by incorporating lines of defense throughout an interconnected network. These technologies are basically analogous to having an antivirus software installed on a personal computer to protect from malicious software. One such technology which was designed expressly for this reason is the Tofino Industrial Security Solution [23], which provides industrial strength security, always-on security modules, and is designed for operation within harsh operating environments. Software such as these are generally expected to adhere to ISA99 standards for security systems [24]. Figure 11 below displays a visual example of the concept of Defense in Depth as applied to cybersecurity in SCADA systems.



HIRSCHMANN
A BELDEN BRAND

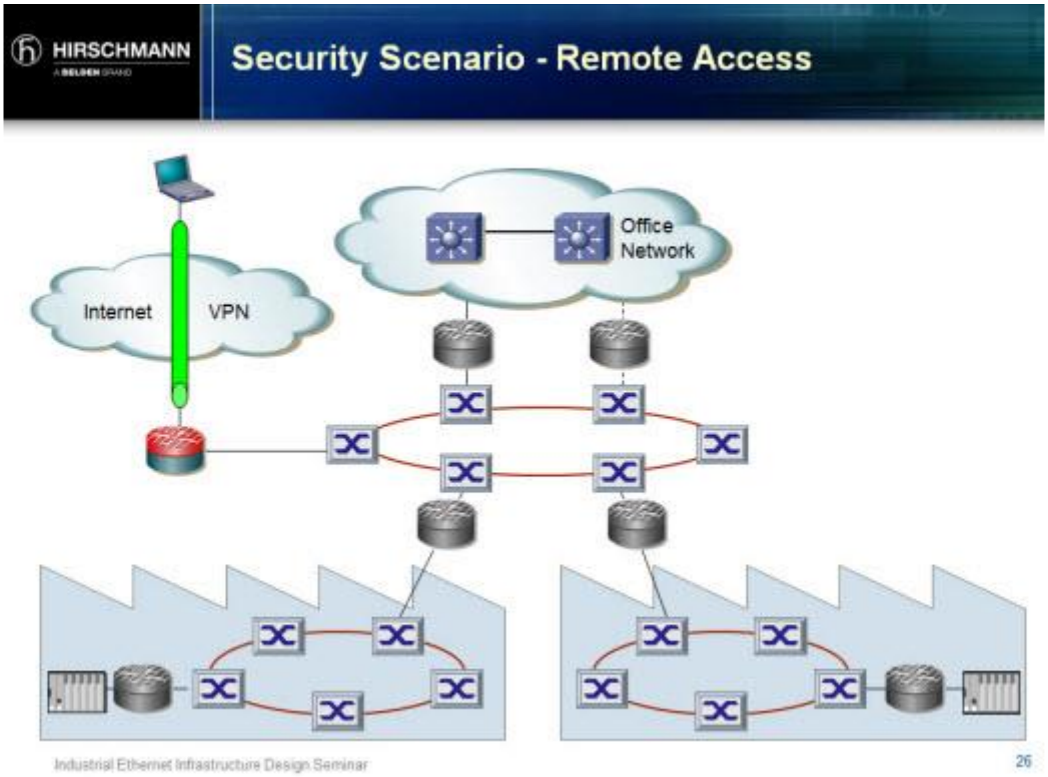
Security Scenario - Defence in Depth

Industrial Ethernet Infrastructure Design Seminar

25

Figure 11. Defense in Depth in SCADA Systems [19]

To address the issue of remote entities introducing malware or inappropriate network traffic to a SCADA system via a network connection, one such solution is to secure the network through the usage of a virtual private network (VPN) [25]. Using a VPN will create an insular network which doesn’t have any sort of remote entry point. Figure 12 below displays the usage of a VPN within a SCADA system context.



HIRSCHMANN
A BELDEN BRAND

Security Scenario - Remote Access

Industrial Ethernet Infrastructure Design Seminar

26

Figure 12. VPN Remote Access with SCADA [19]

There are other, smaller methods to securing a SCADA system. One such method is to frequently perform technical audits of the devices and networks within the system so as to track for new security threats and vulnerabilities. [26] These audits can include but may not be limited to testing for proper data input to and from PLC's and RTU's, respectively, as well as proper physical functionality of the devices, connection errors, and the like. Proper training and preparation of personnel can be key to the continued success of a SCADA system. Personnel should be designated specific roles and tasks to carry out as they relate to the cybersecurity of a SCADA system. [26] A company can establish a SCADA "Red Team" [27] who specifically work to generate possible attack scenarios so they can better be equipped to address these theoretical scenarios. This team thereby is generating specific requirements for cybersecurity. [26] There may exist times in which a system requires changes for some reason. The introduction of these changes can unintentionally cause new network security issues. To mitigate this potential issue, a company can establish configuration management processes which cover the consistently required configurations of both the hardware and software involved in a SCADA system. [26] Finally, in the unfortunate event of a successful cyberattack on the part of some third-party perpetrator, it is necessary to have system backups and disaster recovery plans in place to attempt to reset the system to their previous state after the repercussions of the attack have been dealt with so that the industrial processes can begin anew and so that work can be begun to address the vulnerabilities which allowed for the attack to occur in the first place. [26]

4. Conclusion

In conducting this research project, much has been learned about what industrial control system architectures are and why they are useful. More specifically, this knowledge has been applied to the research of the SCADA control system which uses programmable logic controllers and remote terminal units to automate the control of the physical devices which make up an industrial environment as well as how best to secure any and all vulnerabilities and repel threats to the technology. This information is significant because it shows in an even broader sense than merely the domain of SCADA what control systems are and how they function. It shows how SCADA systems make up the architectural backbones which provided a continued successful operation to so many industrial environments. The extreme importance of these systems thereby highlights the importance of proper, diligently-enforced cybersecurity systems. If important systems such as these which are critical to the operation of physical hardware which are economy-critical are insecure, the company and its industrial environment are thereby compromised, which can lead to costs in the millions in damages. The knowledge of the SCADA system and methods of securing it then can be applied to a number of other control systems. With more time, it would be feasible and worthwhile to explore specific examples of SCADA systems embedded within actual company industrial workplace environments, how they function, and how they are maintained by human personnel. Next, with specific data on the real-world practicalities of SCADA systems embedded within actual environments, one could develop a cost-benefit analysis which compares and contrasts the benefits and drawbacks of using the SCADA system against the usage of other control system architectures.

5. References

[1] Tutorials Point, Control Systems – Introduction, Tutorials Point, Hyderabad, India, January 18, 2017

[2] Gordon Clarke, Practical Modern SCADA Protocols: DNP3, 60870.5 and Related Systems, Newnes, London, England, April 15, 2004

[3] Inductive Automation, What is SCADA?, Inductive Automation, Folsom, California, USA, March 29, 2017, https://inductiveautomation.com/what-is-scada

[4] Machine Design, Engineering Essentials: What Is a Programmable Logic Controller? Informa, London, England, June 1, 2015, http://www.machinedesign.com/engineering-essentials/engineering-essentials-what-programmable-logic-controller

[5] Siemens, SCADA Remote Terminal Units (RTU), Siemens Industry, Inc., Munich, Germany, January 22, 2008, http://w3.usa.siemens.com/smartgrid/us/en/transmission-grid/products/scada-remote-terminal-units/pages/scada-remote-terminal-units.aspx

[6] Wonderware, Human Machine Interface (HMI), Schneider Electric, Lake Forest, California, USA, June 2, 2016, https://www.wonderware.com/hmi-scada/what-is-hmi/

[7] Lifewire, What's a LAN (Local Area Network)?, Lifewire, United States, October 20, 2017, https://www.lifewire.com/local-area-network-816382

[8] Lifewire, What Is a Wide Area Network (WAN)?, Lifewire, United States, November 8, 2017, https://www.lifewire.com/wide-area-network-816383

[9] Unitronics, What is a PLC, Unitronics, Israel, November 6, 2017, https://unitronicsplc.com/what-is-plc-programmable-logic-controller/#

[10] David Bailey & Edwin Wright, Practical SCADA for Industry, Elsevier Science, Amsterdam, Netherlands, June 23, 2003

[11] WhatIs, intelligent electronic device (IED), TechTarget, Newton, Massachusetts, September 28, 2017, http://whatis.techtarget.com/definition/intelligent-electronic-device

[12] Kunbus, Key Technology for Automation, Kunbus, Denkendorf, Germany, July 31, 2014, https://www.kunbus.com/fieldbus-basics.html

[13] Cates Control Solutions, Programmable Logic Controllers (PLC), Cates Control Solutions, Webster, Texas, August 21, 2010, http://www.cates.com/programmable-logic-controllers-plc/

[14] Kalpana Chauhan, Rajeev Kumar Chauhan, Mohan Lal Dewal, Utility of SCADA in Power Generation and Distribution System, 3rd IEEE International Conference on Computer Science and Information Technology, Beijing, China, July 2010, https://www.researchgate.net/publication/235671032_Utility_of_SCADA_in_Power_Generation_and_Distribution_System

[15] ATI Systems, Remote Terminal Unit (RTU), Acoustic Technology, Inc., Boston, Massachusetts, September 25, 2011, https://www.atisystem.com/products/rtu.htm

[16] Schneider Electric, Wonderware HMI/SCADA, Schneider Electric, Lake Forest, California, April 3, 2017, https://www.wonderware.com/hmi-scada/

[17] Schneider Electric, Wonderware Software Makes Machine Performance, OEE and OMAC PackML Easy, Schneider Electric, Lake Forest, California, November 2, 2014, http://blog.wonderware.com/2014/11/Machine-Performance-OEE-OMAC-PackML-Easy.html

[18] Erik Schweigert, SCADA Security Basics: Why are PLCs so Insecure?, Tofino Security, St. Louis, MO, September 12, 2012, https://www.tofinosecurity.com/blog/scada-security-basics-why-are-plcs-so-insecure

[19] Heather Mackenzie, SCADA Security Basics: Why Industrial Networks are Different than IT Networks, Tofino Security, St. Louis, MO, October 31, 2012, https://www.tofinosecurity.com/blog/scada-security-basics-why-industrial-networks-are-different-it-networks

[20] Tim Fisher, USB: Everything You Need to Know, Lifewire, United States, January 25, 2013, https://www.lifewire.com/universal-serial-bus-usb-2626039

[21] Wayne Chung, SCADA security and understanding the risk impacts, CSO, Framingham, MA, May 1, 2013, https://www.cso.com.au/article/460613/scada_security_understanding_risk_impacts_/

[22] Todd McGuiness, Defense In Depth, SANS Institute, Boston, MA, 2001, https://www.sans.org/reading-room/whitepapers/basics/defense-in-depth-525

[23] Tofino, Tofino Industrial Security Solution, Tofino Security, St. Louis, MO, October 27, 2015, https://www.tofinosecurity.com/products/overview

[24] ISA, ISA99, Industrial Automation and Control Systems Security, Research Triangle Park, NC, August 17, 2003, https://www.isa.org/isa99/

[25] Desire Athow, What is a VPN?, TechRadar, New York City, NY, October 9, 2017, https://www.techradar.com/news/what-is-a-vpn

[26] U.S. Department of Energy, 21 Steps to Improve Cyber Security of SCADA Networks, U.S. Department of Energy, https://www.energy.gov/sites/prod/files/oeprod/DocumentsandMedia/21_Steps_-_SCADA.pdf

[27] Chris Peake, Red Teaming: The Art of Ethical Hacking, SANS Institute, Boston, MA, July 16, 2003, https://www.sans.org/reading-room/whitepapers/auditing/red-teaming-art-ethical-hacking-1272