Test Bed Development for a Security Engineered SCADA Laboratory

Stephen Hopkins, Sikha Bagui, Ezhil Kalaimannan, Amitabh Mishra, Bhavyansh Mishra, and Daniel Kelly
Department of Computer Science
University of West Florida
Pensacola, FL 32514 USA

***Abstract*— Supervisory Control and Data Acquisition (SCADA) systems and Industrial Control Systems (ICS) are critical for infrastructure operations, production processes, automation systems, and other automated control systems. SCADA systems are vulnerable to cyber physical attacks from many vectors. The attack surface varies widely. The problem is complicated by the inherent focus on performance, reliability, and safety rather than cybersecurity. The Secure SCADA Framework establishes a security engineered approach evolving SCADA and ICS systems towards a more cybersecure posture. The encapsulating and integrating concepts of the Secure SCADA Framework require development and analysis of implementations achieving the eight framework goals. This work provides a solution for research, design, development, and evaluation of components of a Secure SCADA System. A Security Engineered SCADA Laboratory requires a test bed with which engineering and science designs can be developed. This paper presents a test bed which can model and collect data on simulated attacks, analyze data to evaluate performance, and provide the foundations for a Security Engineered SCADA Laboratory.**

Keywords*— *Cybersecurity, SCADA, Industrial Control Systems (ICS) security, Vulnerability analysis.

I. Introduction

A. SCADA Architecture, Application, and Communication

Electrical engineers have been the lead developers of SCADA systems for over 90 years [1]. These rarely replaced systems often operate for 15 years [2] or more providing high performance, reliability, and safety in many geographies and environments. The SCADA geographies range from isolated rural installations to concentrated facilities in metro area networks and to distributed facilities in wide area networks. The environments include utility systems, control systems (traffic queueing, production lines), and distribution systems (gas, oil, electric) [3]. SCADA systems lowest common denominator is the physical layer device which control a process using sensors, actuators, and simple logic controllers monitoring set points. The remaining architecture includes automatic control and supervisory control layers and may include production or organization layers. The multi-layered architecture implementations commonly run older operating systems, infrequently install software updates, rarely update embedded firmware [4], have controllers with small buffer sizes, and communicate at slow speeds in the range of 9600 bps [5] using one or more of numerous protocols (Fieldbus, PROFIBUS, Modbus, TCP, IP, etc.) [1]. The systems include many machine types, each with its own communication protocol, including master terminal units (MTU), remote terminal units (RTU), programmable logic controllers (PLC), and intelligent electronic devices (IED), human machine interfaces (HMI), workstations, and servers. Communications from the automatic control layer may traverse point-to-point connections, series, series-star, and multidrop connections [6]. The communications are designed to optimize the master-slave relationship between upper layers and the physical layer devices. Installation and operation costs typically drive implementations away from the most efficient point-to-point topology [6]. Users include field technicians, control engineers, vendors, and corporate personnel. The four primary communication functions include data acquisition, firmware download, control functions, and broadcast [5].

B. Current SCADA Vulnerability, Threats, and Mitigation

Historically, SCADA systems were isolated from outside communications such as the internet. A practice of security by obscurity became common place even though many of the devices and protocols documentation are available as open source. These systems focusing on performance, reliability, and safety including multiple users, multiple layers, multiple data communication categories, and many access points are less monolithic and increasingly internet connected [7] including distributed networks, Internet of Things (IoT), and Industrial Internet of Things (IIoT). Architectural [5], security policy, hardware, software [7], and communication vulnerabilities [6], [1, 2, 7] are significant and complex considering the wide range and variability of attack surfaces.

- Architectural: internet connection, life time, local access points, multiple access points, web-based applications [1, 5, 6]
- Security Policy: lagging operating system, security by obscurity, software updates [1, 7]
- Hardware and Software: processing power, buffer size, commercial off the shelf hardware, data processing speed, devices [1, 6, 7]
- Communications: proprietary protocols, real-time performance [1]

The threats are characterized by multiple attack types, attack points, common characteristics, and attacker origination.

- Attack Types: Denial of Service, integrity attacks [7]

978-1-7281-0137-8/19/$31.00 ©2019 IEEE

- Attack Points: web-based applications, corporate computers, supervisory control layer, communications networks, physical layer devices [2, 7]
- Common Characteristics: zero-day buffer, non-prioritization of tasks, database injections, communication protocol [6, 7]
- Attacker Origination: operative type [1]

Several mitigations can be used including firewalls [1], demilitarized zones, virtual private networks, data analysis mitigation [7], modeling and estimation [7], intrusion detection systems [8], protocol redesign [9], and cryptography [1]. The challenge to implementing many of these mitigations, such as modeling and estimation, are the design and processing limits of the current system, such as controller capability and communication protocols. Overcoming these and other limits was the focus of previous research developing a Secure SCADA Framework. The Secure SCADA Framework uses encapsulation and integration engineering design to evolve existing SCADA systems towards a cybersecure system. The Secure SCADA Framework leverages several technologies including 5G cellular communications to protect and speed up inter-device communications, machine learning artificial intelligence to analyze and data, modeling and estimation to estimate future states, and introduces a SCADA trusted computing base (STCB) to secure the physical layer in a similar way to computer trusted computing bases [3].

II. Secure SCADA Framework Implications

A. Secure SCADA Framework Definition

Our previous research produced the development of a Secure SCADA Framework [3]. This paper presents a test bed which can model and collect data on simulated attacks, analyze data to evaluate performance, and provide the foundations for a Security Engineered SCADA Laboratory. The Secure SCADA Framework, Figure 1, focuses on encapsulating and integrating cybersecurity measures into SCADA, transforming the system into a larger computing environment containing security controls for cyberthreats which meet eight goals [3].

1. Implement virtual SCADA device addressing using 5G devices and an addressing server performing memory management similar to a central processing unit (CPU) memory manager

2. Implement a SCADA trusted computing base (STCB) protecting SCADA devices with the highest privileges

3. Protect the STCB through interfaces restricting direct access to high privilege functions

4. Maintain SCADA device slow communication rates, small message packets, and real-time operating requirements by not altering those devices

5. Implement device-to-device encrypted communication channels based on cellular technology

6. Apply information security using encrypted communications and intermediary processors filtering data and commands

7. Address confidentiality, integrity, and availability at all layers

8. Perform machine learning and artificial intelligence techniques, modeling and estimation, and additional cryptography on intermediary devices and servers placed within the communication channels.

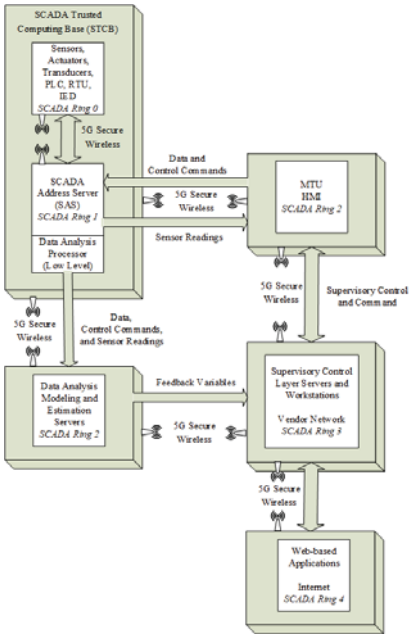

Figure 1. Secure SCADA Framework [3]

B. Test Bed

This phase of the Secure SCADA Framework project includes the implementation of a virtual SCADA device addressing using 5G devices and an addressing server performing memory management similar to a central processing unit (CPU) memory manager. This phase will design, develop, and evaluate components of a Secure SCADA System. This will test the adaptation of cellular devices to SCADA physical layer systems which will communicate securely to cellular device(s) connected to computer servers providing memory management of a set of physical layer devices and communications with each of the physical layer devices. Basically, this phase of the project will include the development of a test bed, model and collect data on simulated attacks, and analyze data to evaluate performance. Development of the test bed provides the primary tool for the foundation of the Security Engineered SCADA Laboratory, the evolving prototype of the Secure SCADA Framework, and the validation environment for production devices.

III. Test Bed Impacts

A. Advantages of Developing this Test Bed

This project implements the foundation of a system which controls access to the physical layer devices and provides a platform for the development of focused machine learning and artificial intelligence processing of physical layer device commands and data. A SCADA modeling and vulnerability test

bed will 1) provide a platform for demonstrating SCADA performance in a research environment, 2) implement consistent threat models and attacks, collect and analyze data to evaluate designs, and 3) provide a repeatable test environment. Integration of higher order processing between vulnerable physical layer devices and upper layer machines provides machine learning and artificial intelligence ability to detect singular and collaborative attacks upon the systems. The encapsulation of communications into a homogenous secure channel through a controlling addressing server reduces the attack points. The adaptation of the encapsulating and integrating technology while retaining existing physical layer and automatic control layer devices retains the level of reliability, safety, and performance of proven SCADA devices. From the applications of this research, we will learn how a Secure SCADA Framework hardens the system from cyber-physical attacks with a cost benefit of avoiding a complete redesign of a working SCADA system.

B. *Encapsulation and Integration Driven Features*

The test bed provides six features which aid the understanding of SCADA functionality, analysis of SCADA performance, and development of security features for SCADA systems including data availability, modularity, control, interchangeability, extensibility, and boxing flexibility. The test bed provides access to data at all levels of the Secure SCADA Framework. The capture and analysis of this data in and of itself and with respect to other data sets within the framework provides the opportunity for knowledge discovery. The test bed design parallels a production system while implementing the functions in a modular construction. Encapsulation and integration are key concepts of the Secure SCADA Framework. The test bed design modularization accommodates these concepts. Design modularity provides the features of control, interchangeability, extensibility, and boxing flexibility. Control is achieved by the ability to change performance at the module level extending analysis of impacts to the system level. Interchangeability is achieved by adhering to interface characteristics and performance between modules and allowing the modules to change function within the constraints of the interfaces. Long term implications of interchangeability are the ability for the test bed to integrate production equipment, such as Programmable Logic Controllers (PLCs), for various components within the test bed. The design focus on encapsulation and integration through modularization provides the ability to adapt new devices between interfaces and insert additional components, such as a SCADA Addressing Server (SAS), between these devices. Boxing flexibility is achieved by the ability to access or deny data at any component of the test bed. Full access to the data provides excellent support for white box testing. Limited access to the parts or all of the data provides graduated support for grey and black box testing.

C. *Key Research Questions*

The expected outcome of the this phase of the research is the development of a system which controls communications to physical layer devices and protects against known attacks. The test bed provides the ability to address several key research questions.

- What model can represent the operation and performance of physical layer devices?
    - What are the range of operations and distributions of physical layer devices?
    - Can this model be extended to the cellular adapted physical layer device designs?
    - What simulations can execute the cellular adapted physical layer device model?
- What is the attack surface of physical layer devices?
    - What is the model of the attack surface of physical layer devices?
    - What are the models of attack methods?
    - How do the physical layer devices respond to attack methods?
    - How do the cellular adapted devices respond to attack methods?
- How can a cellular device attach to existing SCADA physical layer device communications?
- What communication protocol (algorithms and packaging) can be used to translate established SCADA protocols through secure cellular transmissions?
    - What performance loss is experienced using the communication protocol?
    - What addressing design can provide virtual addressing of physical layer devices?
    - How well will the cellular adapted physical layer devices operate the range of operations and distributions of physical layer devices?
- What methods can be used to detect malformed data and commands?
    - How do the methods respond to attack methods?

IV. Development of a Test Bed

A. *Test Bed Architecture*

The test bed is designed to model the SCADA system physical and automatic control layers with respect to goals 1 through 3 of the Secure SCADA Framework. The project goals include

- Develop models of physical layer operations and distributions.
- Develop the model of the attack surface and methods.
- Develop a test bed to establish baseline performance and evaluate responses to normal operation, fault operation, and attack commands.
- Develop cellular adapted physical layer devices.

- Develop a SCADA Addressing Server with virtual physical layer device addressing, data observation and control, and command operation and control.

These project goals can be realized with an architectural model, Figure 2, including components for the process, controller, communication, automatic control layer supervisors, and SCADA Addressing Server. The test bed includes three realizations of the architecture which progressively incorporate the encapsulation and integration driven six features. The three realizations are designed to progress from a foundational SCADA implementation towards a Secure SCADA system designed for the Secure SCADA Framework. The Simple Process implements fixed manual processes with sensors and actuators. The processes are designed to model both discrete and continuous functions similar to production environments. This provides for the evaluation of both types of data as well as control by various frequency rates. The Simple Process includes a state machine programmer, wired/wireless communications channel, and automatic control layer supervisor. The Modeled Process replaces the fixed manual process with a microcontroller containing modeled processes. The Modeled Process can emulate normal processes, fault processes, vulnerability processes, and attack response processes. The Encapsulated Process replaces the communication channels with microcontroller based cellular components which adapt to the existing communication protocols and provide encrypted communications to the SCADA Addressing Server.

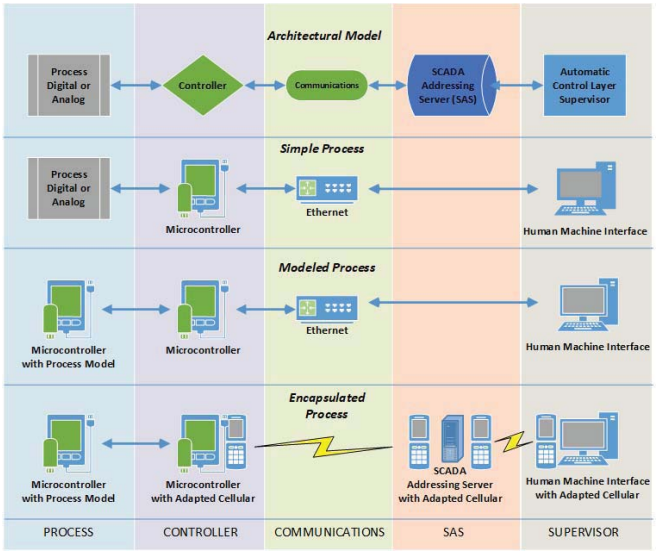

Figure 2 Secure SCADA Test Bed Architecture and Realizations

B. Data Acquisition

Data acquisition is performed at each component level using sensors and data loggers. The sensors include analog and digital measurement devices and displays. The data loggers include microcontroller and computer devices. The data is synchronized, extractable, and available for higher order processing including time-based analysis, statistical analysis, and data mining. The measured data includes analog and digital measurements representing response times, performance, data flow, and system states in normal, attack, and failure modes.

C. Tests and Data Analysis Plans

1) Physical Layer Device Model.

Physical layer devices controlling processes are the foundation of SCADA systems. Although operational physical layer devices could be used for this project, research models of the physical layer device provide the ability to model many different physical layer device performance characteristics. The scope of this research is to design, develop, implement, test, and verify the research physical layer device model. Model in the scope of this task is a functional physical layer device implemented with the ability to vary response time, performance, and data flow. The datalogger implements the ability to monitor and capture data and system state.

2) Automatic Control Layer and Physical Layer Device Attack Vectors, Surface, and Methods.

SCADA physical layer devices can be attacked in multiple ways. Each attack vector defines a path which an attacker gains access, control, and disrupt normal operations. The summation of the attack vectors is an attack surface. Each attack vector is achieved in an attack following certain methods and procedures. The attack vectors of a physical layer device provide one attack surface. The automatic control layer devices communicate with and control physical layer devices. The attack vectors of the automatic control layer provide a second attack surface. The combination of the two layers include additional attack vectors which defines a third attack surface. The combination should include the integration of vendor, maintenance, and backdoor attack points. The scope of this research is to provide automatic control layer command and communication to the research model physical layer devices, define attack vectors for the surfaces, analyze the data and verify research model vulnerabilities match operational device vulnerabilities, and test the research model against the attack vectors.

3) Cellular Device Integration and Encapsulation.

The Secure SCADA Framework replaces all communication channels with secure channels via cellular wireless technology. SCADA includes many diverse communication protocols. Current 4G/LTE and developing 5G technology have features which can provide secure communications channels. The cellular devices will be modified to attach directly to existing SCADA physical devices, tunnel the existing protocol, communicate with an associated cellular device connected the SCADA Addressing Server. The scope of this research is to 1) identify cellular security features to provide a secure communications channel, integrate cellular communications, 2) maintain SCADA physical device slow communication rates, small message packets, and real-time operating requirements by not altering those devices, and allow for SCADA Local Addressing (SLA) which uniquely identifies each physical device / cellular combination.

4) SCADA Addressing Server (SAS).

Implement virtual SCADA device addressing using cellular devices and an addressing server performing memory management similar to a central processing unit (CPU) memory manager. The SAS 1) provides memory management using

SCADA Local Addresses, 2) implements architecture-wide point-to-point topologies, communicates to physical devices through cellular communications channels, 3) controls all communications to the physical devices, secures all access points and reduces the scale of complexity, and 4) identifies malformed data and commands which put the SCADA devices into a singularity or subject them to attacks such as buffer overflow. The scope of this project is to perform goals 1 through 3 of the Secure SCADA Framework.

V. Addressing Limits of a Test Bed

A test bed focused on the foundations of a Security Engineered SCADA Laboratory, the development of evolving prototype of the Secure SCADA Framework, and the validation environment for production devices does have limitations. There are unique production cyber-physical issues which the test bed does not address in its simple form. The test bed is designed to operate in a non-production environment, implements non-production PLCs, and operates at limited scale in order to evaluate multiple approaches to secure SCADA systems. Production environments include unique issues in the perimeter defense posture and environment conditions. The definition of the perimeter varies by implementation resulting in seemingly dissimilar perimeter defense architectures [3]. The test bed is a confined system without a perimeter corresponding to a production environment. Production systems can be subject to temperature, moisture, vibration, and electromagnetic interference extremes. The Security Engineered SCADA Laboratory test bed addresses these limitations using some of the six encapsulation and integration features. Data capture points are designed in all interfaces and modules of the test bed. Evaluation of perimeter defense processes can be tested and analyzed at combinations of the data capture points which represent the desired perimeter. The modular design provides the ability to interchange production equipment into the test bed. Analysis of the production equipment in a production environment allows extending impacts of the environment to the models by way of implementing performance changes into models. Verification and validation of processes between the test bed models and the production equipment integrated into the test bed establish performance which accounts for the environment. The test bed implements microcontrollers to model the processes, controllers, communications, and supervisors in a SCADA system. The microcontroller use combined with the modular design allows for the extension of the test bed to incorporate more components, which addresses scale of a test bed as compared to a production environment.

VI. Summary

Securing SCADA and ICS is critical to the protection of infrastructure, operations, production, automation, and other processes. The Security Engineered SCADA Laboratory test bed development provides the tools to research, design, develop, and evaluate components of a Secure SCADA System.

References

[1] V. Igure, S. Laughter, and R. Williams, “Security Issues in SCADA networks”, Computers and Security, vol. 25, 2006, pp. 498-506

[2] D. Bradbury, “SCADA: a critical vulnerability”, Computer Fraud & Security, Volume 2009, Issue 8, August 2009, pp. 18-20, https://doi.org/10.1016/S1353-4858(09)70078-9

[3] S. Hopkins and E. Kalaimannan. “Towards Establishing a Security Engineered SCADA Framework”, *Journal of Cyber Security Technology*, Accepted, 2019.

[4] S. Gold. “The SCADA challenge: securing critical infrastructure”, *Network Security,* Volume 2009*,* Issue 8, August 2009, pp. 18-20, https://doi.org/10.1016/S1353-4858(09)70078-9

[5] Y. Wang and B. Chu, *sSCADA: Securing SCADA Infrastructure Communications*, Charlotte, NC: Dept. of SIS, UNC Charlotte, 2004, pp 1-13

[6] B. Babu, T. Ijyas, Muneer P. and J. Varghese, "Security issues in SCADA based industrial control systems," *2017 2nd International Conference on Anti-Cyber Crimes (ICACC)*, Abha, pp. 47-51, 2017, doi: 10.1109/Anti-Cybercrime.2017.7905261

[7] V. Do, L. Fillatre, I. Nikiforov, and P. Willett, “Security of SCADA Systems Against Cyber – Physical Attacks”, *IEEE A&E Systems Magazine*, May 2017, pp. 28-45

[8] S. Agrawal, J.Agrawal, “Survey on Anomaly detection using Data Mining Techniques” *Procedia Computer Science*, vo 60, 2015, pp 708-713

[9] R. Czechowski, P. Wicher and B. Wiecha, "Cyber security in communication of SCADA systems using IEC 61850," *2015 Modern Electric Power Systems (MEPS)*, Wroclaw, 2015, pp. 1-7