A Testbed for SCADA Control System Cybersecurity Research and Pedagogy

Thomas Morris  
Mississippi State University  
Box 9571  
Mississippi State, MS 39762  
+01-662-325-3199  
morris@ece.msstate.edu

Rayford Vaughn  
Mississippi State University  
Box 6343  
Mississippi State, MS 39762  
+01-662-325-3570  
vaughn@research.msstate.edu

Yoginder Dandass  
Mississippi State University  
Box 9637  
Mississippi State, MS 39762  
+01-662-325-7502  
yogi@cse.msstate.edu

ABSTRACT
This paper describes the Mississippi State University Supervisory Control and Data Acquisition (SCADA) security laboratory and Power and Energy Research laboratory. This laboratory combines process control systems from multiple critical infrastructure industries to create a testbed with functional physical processes controlled by commercial hardware and software over common industrial control system routable and non-routable networks. The testbed enables a research process in which cybersecurity vulnerabilities are discovered, exploits are used to understand the implications of the vulnerability on controlled physical processes, identified problems are classified by criticality and similarities in type and effect, and finally cybersecurity mitigations are developed and validated against the testbed. The testbed also enables control system security workforce development through integration into the classroom of laboratory exercises, functional demonstrations, and research outcomes.

Categories and Subject Descriptors
C.3 [Special-Purpose and Application-Based Systems] – process control systems.

General Terms
Measurement, Experimentation, Security

Keywords
Testbed, industrial control system, SCADA, cybersecurity

1. INTRODUCTION
University, government, and industry based researchers have begun to develop testbed solutions that model industrial control systems to support cybersecurity research and development in this domain. The majority of testbeds documented in the literature model control systems and their associated networks using various simulation technologies. This paper describes a unique university based testbed which includes commercial hardware and software and includes functioning physical processes to model contemporary control systems found in critical infrastructure.

The testbed includes laboratory scale control systems from multiple critical industries including, petrochemical manufacturing, gas pipeline operation, electricity transmission, factory systems, steel manufacturing, and heating ventilating and air conditioning (HVAC) in the form of 7 industrial control systems built with commercially available hardware and software. The control systems include remote terminal units (RTU), programmable logic controllers (PLC), sensors, actuators, and human machine interface (HMI) software, commonly found in industrial critical infrastructure applications. Each system controls a functional laboratory scale physical process. The physical processes include a storage tank (which models a petroleum storage application), a raised water tower, a factory conveyor belt, a gas pipeline, an industrial blower, and a steel rolling operation, and a smart grid transmission control system.

A remote connection exists to a second facility on the university campus which houses electric transmission substation devices and control center software and systems. The electric transmission substation and control center facility contains protection relays, phasor measurement units, phasor data concentrators, a synchrophasor vector processor, programmable logic controllers, a substation GPS clock, a Real Time Digital Simulator, OSISoft PI Historian.

The combined testbed is used to support university based research and development in support of identifying existing industrial control system vulnerabilities, developing vulnerability taxonomies to identify common cybersecurity deficiencies in need of solutions development, and to serve as a platform for validating research cybersecurity solutions which serve industry and government. The testbed has been successful in identifying significant vulnerabilities.

The combined testbed is also used for pedagogical purposes. First, a graduate course dedicated to industrial control system cybersecurity concepts has been developed. Second, concepts and experiences learned from research activities using the testbed have been integrated into multiple other classes. Finally, researchers are currently developing material for a series of workforce development short courses.

2. RELATED WORKS
The Idaho National Labs (INL) National SCADA Testbed Program is a large scale testbed program dedicated to control system cybersecurity assessment, standards improvement, outreach, and training [1]. The INL SCADA Testbed includes a full scale electric power grid, a wireless testbed facility, and a
Cyber Testbed is available to support testing of firewalls and virtual private networks (VPN). A European SCADA Testbed has been proposed to provide real world testing facilities for SCADA manufacturers, academic researchers, and other stake holders [2]. The authors are currently working with collaborators in Australia to establish a testbed there.

Simulated testbeds [3] [4] offer a low cost means to model industrial control systems and the effects of cyber security attacks on such systems. Simulated testbeds lack the ability to completely model the interactions of control system components. Testbeds built from commercial hardware and software are typically limited in size and scope. In [5] Fovino et al. provide details of a laboratory used for SCADA cyber security research which includes components from a functional Turbo-Gas Power Plant (modeling a type of electric power generation system). In [6] Hahn et al. document a testbed which models two electric substations connected to a control center. The British Columbia Institute of Technology (BCIT) houses a SCADA testbed known as the Industrial Instrumentation Process Laboratory. The BCIT lab includes a fully operational distillation column, evaporator, a batch pulp digester, a chemical blending reaction process, and power boiler [7].

3. TESTBED COMPONENTS

The physical processes and control systems in the testbed models systems found in multiple critical industries including electric power transmission, gas distribution, water storage and distribution, manufacturing, mining, and steel manufacturing. The control systems in the testbed are divided into 2 categories based upon communication type: 5 systems use serial port communication and 2 systems use Ethernet communications.

3.1 Serial Port Control Systems

The serial port control systems in the testbed include a water storage tank, a raised water tower, a factory conveyor belt, a gas pipeline, and an industrial blower. These 5 control systems represent a diverse set of industries and control schemes.

A single HMI implementation is used to control all 5 serial port control systems. Separate screens are available to monitor and control each individual control system. All control systems may be operated simultaneously to simulate a larger system.

Figure 1 shows pictures of representative control systems and associated HMI.

The HMI shown with the serial port control systems is GE/Fanuc iFix. The GE/Fanuc iFix HMI supports 3 communication protocols MODBUS ASCII, MODBUS RTU, and DNP3. All three communication protocols are primarily command response based. A master node, in this case the HMI, sends commands to slave nodes, the individual RTU, which execute the command and then provide a response. Commands include requests for information such as reading values stored in system registers and commands to change system state.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.

CSIIR ‘10, October 12–14, 2011, Oak Ridge, TN, USA.
Copyright 2011 ACM 1-58113-000-00/0010…$10.00.

The HMI forwards MODBUS commands to the master terminal unit (MTU) which in turn forwards commands to the RTU. The MTU is configured as a repeater. The MTU includes 2 EIA-232 UART. The first UART is connected by serial port cable to the HMI host. The second serial port UART is connected to an industrial 900MHz radio. Commands from the HMI are received on the HMI port and forwarded to the radio port. The industrial 900MHz radio is also a repeater which wirelessly broadcasts commands and responses to other radios in the network (there is one radio for each RTU). Responses from RTU are handled in a similar manner except information flows in the opposite direction.

Figure 1: Representative Testbed Control Systems and HMI

The MTU and RTU are identical Control Microsystems, Inc. SCADAPack LP PLC. Each PLC is controlled by firmware. Firmware may be written as Ladder logic, in ANSI C, or may be a combination of both. As mentioned above, the MTU PLC is configured as a repeater; the MTU copies commands and responses received from the HMI port to the radio port or vice versa. Each RTU PLC contains custom ladder logic to control an individual physical process.

RTU ladder logic for the 5 serial port control systems use a common configuration. RTU include input registers, also known as setpoint registers. The HMI software makes changes to setpoint register values to control the physical process. Common setpoint register types include, mode settings, actuator (valve, breaker, switch) settings, and process parameter settings (maximum and minimum valves for controlled process parameters, PID settings, etc.). RTU also include output registers. Output registers contain measured values from the physical process and state information for actuators in the control system. Output registers may be connected to analog inputs to the RTU, digital inputs to the RTU, or be driven by ladder logic or C firmware.

Each serial port control system is configurable. The testbed includes Telepace ScadaPack Programming Software to modify ladder logic and Telepace C Compiler to compile C programs for use on the Control Microsystems, Inc. New monitoring and control logic associated with new inputs and outputs can be added using ladder logic. The HMI screens can be configured to add or remove visualizations or controls. C programs can be used to implement control algorithms or to make network stack changes. SCADAPack LP PLC.
Gas Pipeline - The gas pipeline control system models a gas pipeline used to move natural gas or other petroleum products to market. Cyber penetration of control systems monitoring and controlling a gas pipeline control systems can lead to loss of visibility and loss of control of the gas pipeline. Both cases may lead to financial loss by affecting billing systems and may lead to physical harm to the gas pipeline and to individuals in the vicinity. The gas pipeline control system contains a closed loop gas pipeline connected to an air pump which pumps air into the pipeline. A manual release valve and a solenoid release valve are available to release air pressure from the pipeline. A pressure sensor is attached to the pipeline which allows pressure visibility at the pipeline and remotely on an HMI screen. In automatic mode a PID control scheme is used to control pressure in the pipeline. The PID control variable optionally may be turning on/off a pump or open/closing a relief valve. Alternatively, a manual mode allows an operator direct supervisory control over the pump state and relief valve state to manually control the system.

Storage Tank – The storage tank control system models chemical storage tanks found in the petrochemical industry, water tanks found in water distribution, and storage tanks found in many forms of manufacturing. The storage tank control system contains a storage tank (which holds water in the lab), a pump to add water to the tank, a gravity fed manual relieve valve which allows water to flow out of the tank, and a sensor which provides the water level in the tank as a percentage of total capacity. In automatic mode, an on/off control scheme is used to control the pump state to keep water between high and low setpoints which are configurable by an operator using the HMI. A manual mode is also available to allow supervisory control of the water pump. In both modes an alarm will sound if the water level is outside an operator defined range.

Raised Water Tower – The raised water tower control system models water towers used to provide water pressure in water distribution systems. The raised water tower control system contains storage tank which holds water, a pump to add water to the tank, and four fixed sensors which detect the presence of water at approximately 20, 40, 60, and 80% water tank capacity. Water runs out of the tank via a manual relief valve which can be adjusted to simulate variable usage rates. In automatic mode, an on/off control scheme is used to control the pump state to keep water between 40 and 60% full. A manual mode is also available to allow supervisory control of the water pump. In both modes an alarm will sound if the water level exceeds 80% or drops below 20%.

Factory Conveyor – The factory conveyor belt control system models conveyor belt and sorting control systems used to in the manufacturing industry. The factory conveyor belt control system contains a vision system to detect the color of pucks which travel on the conveyor. After color detection, pucks are sorted by moving a mechanical gate. A manual mode is available to allow supervisory control of the motor direction and mechanical gate state.

Industrial Blower - The industrial blower control system models an industrial blower used to force air through an exhaust system. Similar industrial blowers are used to evacuate gasses from mines, in heating, ventilating, and air conditioning (HVAC) control systems, and in chemical exhaust hoods. The industrial blower uses a PID control scheme to control the air flow into an exhaust pipe. The PID control variable is the percent open of an air damper. A manual mode is available to allow supervisory control of the damper position.

3.2 Ethernet Based Control Systems

Many modern control systems use Ethernet-based communications infrastructures. These Ethernet networks may be electronically isolated networks dedicated to control system interactions. Such systems are said to have an air gap. Air gapped systems are believed to be more cyber secure due to their isolation. However, air gap systems can still be vulnerable to penetration through unintended network connections or through other attack vectors such as infected USB drives. Many control system networks are not electronically isolated. Such networks may have connections to corporate intranets and also to the internet. The trend of using Ethernet-based communications for control systems has led to increased cybersecurity awareness and research and development in the control system domain.

The testbed includes an Ethernet network which connects two control systems: a steel rolling operation and a smart grid transmission control system.

Steel Rolling Operation - The steel rolling operation control system models a four high stand steel rolling operation. These steel rolling operations are used to press sheet metal to add strength via strain hardening and to improve surface finish. A variable frequency drives (VFD) is controlled by the PLC to roll the steel. To fit in a laboratory the VFD turns a simulated load (a large weight). The steel rolling operation includes modes to load simulated rolls of steel onto rollers and to advance and reverse steel through the steel rolling operation. Manual modes are available to control the VFD.

Smart Grid Transmission System - The Smart Grid transmission control system provides a second environment for research in industrial control system cybersecurity. A Real Time Digital Simulator (RTDS), protection relays, and phasor measurement units are connected to the RTDS in a hardware-in-the-loop configuration. The RTDS is used to simulate bulk power scenarios. The protection relays can be configured to monitor bus voltage, current, frequency, and phase conditions to detect circuit faults. Phasor measurement units continuously measure bus voltage, current, and phase, and transmit measurements to phasor data concentrators. A commercial energy management system is used for wide area monitoring and control.

4. PEDAGOGY

The testbeds described in this paper have had a significant pedagogical impact at the university. Integration into the classroom allows the testbed to provide a workforce development function, prepares graduate students for research activities, and raises the profile of this research area with students.

First, a graduate course has been developed to teach industrial control system cybersecurity concepts. This class is available to students across multiple disciplines including all fields of engineering, computer science, and management information systems. The testbed described in this paper has been used to support development of classroom material, to provide live demonstrations of control systems in use, to provide live demonstrations of control systems under cyber attack, and for laboratory exercises for students. Second, concepts and experiences learned from research activities using the testbed have been integrated into multiple other classes. Classes which added material related to the SCADA testbed include Data
Communications and Computer Networking, Software Engineering Senior Design, Introduction to Software Engineering, Information and Computer Security, Operating Systems, Power System Operation and Control, Power System Modeling and Simulation, and Cryptography and Network Security [9]. Finally, researchers are currently developing material for a series of workforce development short courses. The electric utility industry currently has an aging workforce and is working to replace retiring workers. Additionally, the emergence of the Smart Grid is changing the business practices at utilities. Both these factors combine to create a need for short courses to train existing utility employees and prepare new employees.

5. RESEARCH THRUSTS

Research and development in the two labs has primarily included software and network cybersecurity. The testbed enables research by allowing researchers first to investigate cybersecurity vulnerabilities on functional control systems. Researchers typically implement exploits and attack the systems in the testbed to understand the implications of the vulnerability. Vulnerabilities can be ranked by criticality and classified by similarities in type and effect. Researchers then develop cybersecurity mitigations for vulnerabilities which are implemented and validated against the previously generated exploits using the testbed.

Specific software related projects include laboratory research to identify common human machine interface (HMI) vulnerabilities. Results from the study of one HMI revealed a password recovery vulnerability, insecure transmission of remote authentication credentials over a network, and the ability to bypass authentication routines to elevate privilege [9]. HMI passwords were on the HMI host in an insecure manner. Passwords were stored after XOR with a fixed key. The XOR process obfuscated passwords, however, the fixed key is recoverable with a chosen plaintext attack. Further examination of the same HMI found that the mechanism to support remote authentication passed the password file over the network encrypted in the manner described above to the remote client attempting to login. This practice provides an easy means for attackers to access the password file and enables the aforementioned password recovery vulnerability. Finally, review of the studied HMI revealed that the HMI did not include mechanisms to prevent replacement of executable code related to the HMI from outside of the HMI running context. Researchers leveraged this vulnerability to replace a DLL which included authentication routines with an altered copy which bypassed all authentication checks and gave all users elevated privileges. These vulnerabilities were reported to the software developer and to US-CERT as VU#310355 US-CERT.

A Snort plug-in has been developed to allow Snort to monitor and analyze MODBUS RTU and MODBUS ASCII traffic. The software can run on an existing PC connected to the serial link, such as on the PC hosting the human machine interface software. The software can also be run on single board industrial computers and placed in an inline or tap configuration to monitor MODBUS traffic. In passive mode Snort analyzes traffic for matches against a predefined set of rules. Packets which match rules are logged for review off line by a network or system administrator. In inline mode Snort acts an intrusion prevention system. Special rules, drop rules, are used to detect network traffic which should be dropped. The Snort plug-in has been tested with rules from Digital Bond, Inc. Additionally rules have been developed to detect and prevent denial of service attacks, response injection attacks, command injection attacks, and reconnaissance attacks. The testbed includes a Mu Dynamics MU-4000 Analyzer, a network tester used to test network appliances for denial of service and protocol mutation vulnerabilities.

6. CONCLUSIONS

The Mississippi State University (MSU) SCADA Security Lab and the MSU Power and Energy Research Lab form a distributed and unique testbed for industrial control system cyber vulnerability discovery and solutions research. The labs are built with commercial hardware and software devices from multiple vendors. The testbed includes commercial equipment and software to monitor and control laboratory scale physical processes from multiple critical infrastructures. The testbed is used for pedagogical and research purposes.

7. Acknowledgements

The authors wish to thank Mr. John Gordon of Control Systems, Inc. of Montevallo, AL, for his assistance in designing and manufacturing the testbed control systems described in this paper.

8. REFERENCES


