Industrial Control Systems Security Testbed

Emrah Korkmaz\textsuperscript{1,2}, Andrey Dolgikh\textsuperscript{1}, Matthew Davis\textsuperscript{1}, and Victor Skormin\textsuperscript{1}
\textsuperscript{1}Electrical and Computer Engineering
Binghamton University, Binghamton, NY 13902 USA
Email: \{ekorkma1,adolgikh1,mdavis7,vskormin\}@binghamton.edu
\textsuperscript{2}Institute of Defense Science, Turkish Military Academy, Ankara 06654 Turkey

\textbf{Abstract}—Cyber-attacks on critical infrastructure have been a growing concern to government and military organizations. This paper aims to study the impact of cyber-attacks on a SCADA system. To perform this research, a cyber-physical testbed emulating power generation station is designed. It contains power generation units, real-time programmable logic controllers, drives, HMI and supervisory computers. The testbed implements the process monitoring/data collection, typical for an industrial power facility. This data facilitates the deployment and analysis of several approaches for exposing different attack types and the likely impact of cyber attacks on the testbed.


I. INTRODUCTION

Cyber-attacks against critical infrastructures have been an increasingly important concern when supervisory control and data acquisition (SCADA) systems are connected to the external or internal networks.

Many envision that SCADA systems may be operated through internal networks without being connected to enterprise networks. However, this assumption is not always true in cyber-physical systems, which obtain advanced computing services and communication information through enterprise networks [1]. Furthermore, cyber-security assessment for many critical infrastructures has not been paid necessary attention until recently. However, recent studies demonstrate that cyber attacks can create extremely dangerous circumstances for industrial control systems [1], [2], [3].

The 2015 Dell Security Annual Threat Report [4] shows worldwide SCADA attacks increased from 163,228 in 2013 to 675,186 in 2014. This report demonstrates that cyber-attacks on SCADA systems grew dramatically in 2014. Additionally, 51,258 attacks occurred in the US, which is the third utmost number of attacks per nation in the world. Thus, existing vulnerability of cyber-physical systems should be considered as a large security gap in the national infrastructure.

To prevent and mitigate cyber-attacks, security vulnerabilities of SCADA systems must be investigated. However, most SCADA attacks are unreported because the companies that were exposed to cyber attacks are unwilling to discuss their data breaches that typically contain proprietary information, including financial and personal data [4]. It also shall be realized that operational industrial facilities are not suitable for any experimentation, and many technical properties of their SCADA facilities are strictly proprietary. This reality, justifies development of completely secure and isolated testbeds offering a controlled environment for various experimental studies aimed at the detection and evaluation of cyber vulnerabilities.

In this research, a real-time cyber-physical testbed based on power generation is introduced. This testbed emulates technologies that could be observed in the critical infrastructure, and offers static and dynamic data enabling users to observe the phenomena indicative of normal operation of the facility and its operation under various cyber attacks.

This paper is organized as follows. In Section 2, we describe state-of-the-art testbeds recently built by other universities and laboratories. In Section 3, we explain testbed design and components in detail. In Section 4, our data collection process is presented. In Section 5, we introduce proposed experiments that can be deployed in our testbed. Finally in Section 6, offers the conclusion.

II. RELATED WORK

Cyber-physical systems are commonly available all over the world. They can be used in the various critical national energy infrastructures (e.g. nuclear, gas, oil plants, chemical). However, it is impractical to test real cyber-attacks on these systems without disrupting their routine operation. Thus, it is crucial to develop cyber-physical security (CPS) laboratories to investigate cyber-attacks. To make secure and robust CPS work spaces, several laboratories have been built by universities and national laboratories.

National SCADA Testbed (NSTB) is a national program that combines state-of-the-art systems to research and discover critical security vulnerabilities in the SCADA and distributed control systems (DCS)[5]. The NSTB is developed by miscellaneous labs and industrial control systems (ICS) vendors including Idaho Critical Infrastructure Test Range, Sandia Center for SCADA security, Pacific Northwest Electricity Infrastructure Operations Center, Oak Ridge, and Argonne.

As a part of NSBT, Idaho National Laboratory (INL) has been developed based on cyber-security assessments of national DCS and electrical substation automation components [6]. To accomplish this goal, INL has carried out projects with an electric utility vendor to assess and analyze cyber-security vulnerabilities of electrical substations. Sandia National Laboratory (SNL) is also focused on CPS threats and impacts in electric power systems, programmable logic controllers, and communication systems for NSTB [7]. It has the ability to simulate cyber attacks and defend against them, as well as to develop security frameworks for ICS.

There are also different SCADA cyber-security testbeds developed by universities. In recent research, cyber-security assessment has been increasingly used by researchers on smart power grids. In [8], the Trustworthy Cyber Infrastructure for Power Grid (TCIP) was developed by the University of Illinois.
under the Information Trust Institute. The physical system was created virtually using the PowerWorld server which simulates a real-world power microgrid. The Real-time Immersive Network Simulation Environment (RINSE) is integrated to the CPS system. By using RINSE and realistic network simulations, cyber-attacks and cyber-defense can be tested in this virtualized physical environment.

In [9] and [10], the authors developed a PowerCyber testbed, which is composed of industrial SCADA hardware and software, a virtual 9-bus power system, and networking components. This testbed has been trained to detect cyber-attacks. The Automatic Generation Control algorithm is utilized to investigate impacts on measurements and control directions when a cyber-attack is launched.

Chen et al. have the capability to research cyber security vulnerabilities on the smart power systems under the support of Texas A&M University [2], [11]. In this testbed, a power system simulation is created by using the Real-Time Digital Simulator, LabVIEW and PXI modules, and intelligent electronic devices (IEDs). The Testbed for Analyzing Security of SCADA Control Systems (TASSCS) has also been evaluated to investigate cyber-attacks [1]. This testbed, utilizing PowerWorld simulation and OPNET tools, was developed at the University of Arizona with the intent to detect and protect against cyber-attacks on a virtualized physical system.

A different testbed approach is mentioned, which is slightly similar to our design, by [12]. While many researchers develop virtual power systems by using PowerWorld, Favino et al. implemented real programmable logic controllers (PLCs), remote terminal units (RTUs), sensors, and actuators to the simulation platform. In this way, security problems based on the real integrated control systems can be detected and identified by using different simulated attacks.

Fig. 1. Cyber-Physical system testbed diagram

III. TESTBED DESIGN AND COMPONENTS

Our research group at the Network Core, Binghamton University has several facilities ready to test industrial cyber-physical systems. The testbed consists of real industrial equipment (PLCs, motors, generators, sensors, etc.) and is equipped with necessary monitoring tools. Furthermore, if the need for processing of large volumes of raw data appears, the Binghamton University Compute Cluster (BUCC) can be utilized.

Particularly, components of our cyber-physical SCADA platform can be defined as follows:

1) Programmable Controllers; Programmable controllers vary from very small to quite powerful devices to meet the requirement of users [13]. In our research, we have tried to test the most commonly used and different types of PLCs found in the industrial control systems because they are all open targets to the cyber-attacks. Thus, two different types of PLCs have been set up in our testbed: Allen Bradley ControlLogix, which is an advanced controller, and Allen Bradley Micro850 PLC controller. The ControlLogix is quite new technology in modern automated systems that has the capability to house multiple controllers for the system or network. We utilized a 4-slot ControlLogix and inserted a 1756-L61 controller into the ControlLogix chassis to make multiple control decisions.

The ControlLogix can be programmed via multiple languages: ladder logic diagram, sequential function, function block diagram, and structured text. Rockwell Automation's RSLogix 5000 programming software has been used to create ControlLogix programs. We have utilized ladder logic diagram and function block diagram programming languages to control and display our cyber-physical testbed. Ladder logic diagram is a kind of graphical programming language that enables programmers to edit and monitor controlled tags on the ladder rung. It is a cut-and-dried programming language for PLC engineers. The second of the PLC languages is the function block diagram (FBD) that we utilized in the PLC code. The FBD is the newest PLC coding technique that is used for the first time in the ControlLogix family. Instead of creating multiple ladder rungs in the PLC code, a single FBD can be introduced. In our PLC code, FBD is created to adjust PID parameters of the blower motor. Correspondingly, the blower motor parameters can also be tuned with a few lines of ladder logic.

On the other hand, the Micro850 is linked to the testbed separately because it has no direct connection to the ControlLogix. The related ladder logic diagram of the Micro850 is programmed by Rockwell Automation Connected Components Workbench Software. This software is not only the programming software for the Micro850, but it also enables us to program the PowerFlex modules, which drive the motors.

2) Physical System; Basically, the physical system on the testbed is created to detect, mitigate, and defend against cyber-attacks on power generation based systems. In the testbed, two power generation units have been used as shown in Figure 2.

Firstly, a 0.25 HP 3-phase AC motor and a 0.33 HP permanent magnet DC motor are connected via a coupling tie-in shaft as shown in the right side of Figure 2. The DC motor is operated as a generator which has the capability to generate voltages approximately within the range of 0-400 Volts. The generated voltage is controlled with the PowerFlex 525 AC Drive. The PowerFlex enables the operators of the testbed to control motor parameters (i.e., voltage, speed, torque, position, etc.) on the programming stations [14]. Since the generated voltage is high, single-phase loads are connected to the DC motor to protect the motor from overload conditions.

The second power generation unit is created based upon air
handling design as shown in the left side of Figure 2. It is established by using a 3-phase AC blower motor and a 12-volt DC blower motor. The AC motor is utilized to drive the DC motor so that it generates electricity. The air which is supplied by the AC motor, has been used directly to energize the DC motor. The second generation unit produces small voltages between 0 to 12 volts so any electrical load connection is not considered on the generation unit. Additionally, the PowerFlex 525 AC Drive is used to drive AC motor. In this way, the embedded EtherNet/IP on the Powerflex enables us to change and control desired control values throughout the SCADA network.

![Motor pairs](image)

**Fig. 2. Motor pairs simulating physical process**

(3) **SCADA-HMI;** Human machine interface (HMI) systems allow operators to access the control system by using visualization devices. In the testbed, a private computer with LCD monitor has been used to supervise control tags. By using HMI, PID parameters of the 3-phase DC-motor are able to be tuned. Furthermore, the operator is able to adjust and observe realtime output voltages via the HMI screen. To build, monitor, and control the HMI system, the Proficy HMI/SCADA - iFIX software is used. This supervisory monitoring software enables us to leverage more reliability, flexibility, and scalability in our system [15].

(4) **Communication Infrastructures and Software;** The communication between the controllers, PowerFlex, and HMI Desktop is established using Rockwell Automation Company’s EtherNet/IP Modules which can be used on the ControlLogix chassis. Moreover, communication of all networked devices has been bridged by RSLinx Enterprise [16]. The RSLinx Enterprise by Rockwell Automation is a well-known and commonly used communication server in critical infrastructures that enables us to share networking data between the physical system, controllers, and network devices on the testbed. This network traffic between components of the testbed is monitored by Wireshark network packet analyzer.

(5) **Lab Network Testbed;** Cyber-physical attack/defense scenarios, penetration testing of the testbed technology, and overall level security can be qualified with the help of the Binghamton University computer security testbed (BU-Testbed). The experimental BU-Testbed for information security research was created at BU under two Air Force grants [17]. The network testbed offers a secure, controlled environment for experimental analysis of the efficiency of various intrusion detection/mitigation and computer forensics systems. It allows for staging large scale experiments with real malware on thousands of interacting heterogeneous nodes. The testbed provides effective ways to collect data representing the network and software operation and it facilitates secure time sharing of the hardware among different research projects. Its enhanced security is achieved by separation and hardening of the core services. To provide necessary physical security the facility is installed in a secure isolated room at the campus datacenter.

**IV. DATA COLLECTION**

The testbed is aimed at fusing the statically available environment information (such as electronic data sheets, electric plans, PLC program code, etc.) and the logging information available at run-time. The final result of the technology is the ability to auto-generate and enforce the security policy for the manufacturing floor.

Most industrial manufacturing systems have and produce an abundance of structured and unstructured data that can be used to improve the security of the system. We can classify such source data into two types: first, static data representing the design of the system (equipment description, wiring diagrams, etc.); second, dynamic data representing current running instance of the industrial system with all its parameters (motor/generator temperatures, PLC state, network traffic, etc.). From the formalization point of view these two types of data require different handling.

In our case, we have identified the data collection process according to the availability of data in the testbed. This process can be represented through static and dynamic data compilation.

**A. Static Data**

Static data is usually stored in organized human readable text, machine readable text, and binary files. Machine readable file formats do not represent a significant challenge to read and provide a substantial amount of information about the corresponding manufacturing facilities. Below we list types of static data that are accessible from our testbed (See Figure 3).

- **Device datasheets;** Many industrial manufacturers want to fabricate user-friendly devices. Hence, critical infrastructure control device datasheets are freely available on the internet to help clients. Datasheets of programmable controllers, motor drives, and Ethernet/IP Modules are utilized to reach the static data of cyber-physical testbed. For example, the PowerFlex datasheet allows us to reach manufacturer related information such as output voltage range, frequency range, and overload capabilities of each of the motors.

- **Electric diagrams;** This information can be reachable through the electric diagram of the cyber-physical testbed, which is connected to the lab outlets.

- **Network diagrams;** In the cyber-physical testbed, network diagrams between the controllers, HMI computer, and PowerFlex facilitate us for appropriate data collection.

- **Functional Specifications;** This data type represents the requirements of the power generation process which are basically in human readable format. We have specified how the power generation process should be proceeded.

- **PLC code;** Controllers could be thought of as mini-computers. Thus, uploaded, downloaded, and created PLC
code is easily reversible into original source code and can be utilized for cyber-attacks.

B. Dynamic Data

Dynamic data can be intercepted from the running machinery in a variety of computer readable formats. Below is the list of dynamic data observed through PLC code modifications:

- **Industrial network protocol messages**: This information is obtained through current status or changes in state of the hardware or software of the testbed. Messages describe changes in the status of individual hardware units, actions performed by individual PLCs, warnings and errors, etc.
- **Network activity logs**: These logs are built from the control network traffic monitoring. The following information can be mined from these logs: network identity and connectivity graphs, as well as industrial protocol control message dependency graphs.
- **Tracking of changes**: All changes introduced by an authorized user to control equipment are recorded and reported to the system.

V. PROPOSED EXPERIMENTS

As mentioned in the introduction, traditional SCADA systems are not designed with the highest cyber-security priority. Many industrial control systems are designed to provide a high level of system availability and operational resilience. Low cost has an important role in this process. In addition, other operational requirements, which are environmental priorities and human safety, are considered as the main priorities. [18]. However, building SCADA systems based on cyber-security assessment is not a main concern. Due to this negligence in developing secure cyber-physical system designs, the SCADA systems could be exposed to cyber-attacks.

We designed a testbed that enables us to perform risk analysis of possible cyber-attacks towards real PLCs, drives, operator’s (HMI) computer or programming station, or network. Vulnerability assessment based on a data collection process can be performed by simulating and emulating real world cyber-attack scenarios. In this section, practicable cyber-physical attack scenarios on the testbed are explained. These scenarios can be classified into four different categories:

A. Network Monitoring and Attacks on Networks

**Man-in-the-middle attacks (MitM)**: MitM is a well known attack type that can be done by eavesdropping of a network. The attacker captures transferred exchange packets between sender and receiver devices through sniffing network traffic. The attacker can poison the Address Resolution Protocol (ARP) caches, change sequence number of packets, and ultimately can keep the network connection synchronized while injecting packets [19].

In order to carry out successful MitM attack on our SCADA system, the attacker computer is deployed on the testbed environment and the MitM attack can be penetrated into the network between different testbed components. MitM attack can performed based on poisoning of ARP packets between operator computer, programmer station, PLC, and PowerFlex drives. As a result of a MitM attack, the attacker might cause the following changes on the testbed:

- Static data collection process demonstrated to us that the requirement specifications of every physical component can be forced to change in the testbed. These modifications in the testbed can lead to physical damage of the
equipment. For instance, it is demonstrated that motors on the testbed have a nominal frequency operating limit. This frequency limit can easily be manipulated and increased dramatically through a MitM attack so the augmented frequency causes an increase in the speed of motor shaft or blower motor and alters the generated voltage. Basically, this means that the increased speed causes dangerous overvoltage production and may lead to a crash of the system.

- We have demonstrated that the attacker can easily halt power generation in the testbed. This problem can be thought of as an insignificant stop; however, even a short breakdown in the power generation units could engender serious catastrophic consequences. If the testbed could be thought of as a simplified small part of a power grid distribution system, this fleeting power-cut would cause blackouts and an extreme loss of economy for industrial power plants and consumers.

Local DNS poisoning; The new technological progressions currently enable system operators to use IP based mobile devices (laptops, smart phones, tablet, etc.) on the industrial control systems. While these remote controlled devices have a lot of benefits, such as preventing SCADA systems from sudden failures, they might become a target of cyber-attacks over the internet.

The testbed network also would be facilitated to carry out local DNS poisoning based on phishing attacks. Such attacks are performed by poisoning of local DNS through a rogue access point, when an operator or user types a URL address in the computer’s internet browser [20]. These attacks on critical infrastructures generally are constrained to within the SCADA network because internal SCADA networks have no access to the external internet. However, due to the unauthorized internet access by programming station users or operators, a computer can connect to a malicious web portal.

In this way, the attacker can create two consequences on the testbed [12]:
- Attacker can provide a fake picture of the controlled PID parameters and desired output voltage on the HMI computer screen.
- Attacker can acquire credentials of the operator that enables direct access to the testbed.

B. Network Congestion and Delays Affects

Denial of Service (DOS) attack: Our experimental setup could be used to analyze the behavior of the SCADA network when Denial of Service attacks are carried out. These attacks can likely be successful for critical infrastructures that have connection to the external internet. For instance, power generation and transmission infrastructures which use wide area monitoring, protection, and control (WAMPAC) systems to improve grid stability can be the target for this attack. With this attacking technique, SCADA infrastructures can lose connection to the external network and therefore the attacker may cause potential disruption or stoppage of the SCADA system.

In the testbed, the attacker could increase data-packet-flow severely on the SCADA server using fake service requests which include victim IP addresses. Basically, the SCADA server tries to reply to and overwhelming number of packets that come from attacker side. As addresses are forged, the SCADA server cannot obtain any particular information and thus connection will stop with a timeout [21].

C. Attacks on Controllers, Sensors, and Drives

The attacker can achieve unprecedented levels of control over the SCADA system by subverting the controllers, sensors, and drives. The attacker can achieve this scenario in two different ways over the network: (1) By injecting of malicious software on internal or external network. (2) By creating firmware modification attacks

Malicious software injections; These attacks aim to disable process control systems by causing computer epidemics [17]. To launch those attacks, computer malwares such as worms, viruses, trojans, etc. can be injected into the industrial control systems.

Such malwares on the testbed could infect specific SCADA components that may include:
- ControlLogix/Micro850; so that viral infection disables SCADA controllers.
- PowerFlex-525 devices; so that power generation can be aborted via specific malwares.

With this attack type, the attacker can cause dangerous circumstances on the testbed. Based on the data collection process, specific limits of the PowerFlex drive can be obtained and relevant malwares could be written. For example, the PowerFlex drive has a voltage regulator that prevents users from undesirable overvoltage issues. However, the device could not be stopped when actual deceleration times is longer than commanded deceleration times [14]. The attacker can utilize this information and program malware to carry out on the drive.

**Fig. 4. Firmware modification attack**

Firmware modification attack; This attack type can be exemplified by the notorious StuxNet worm which is created to target critical control infrastructures. This attacking method operates so that until their malicious functionality is implemented, the worms coexist peacefully with the host performing benign exploratory functions [?]. The attack implementation can be seen in Figure 4. Firmware modification attacks can be achievable against embedded SCADA devices, thus PLCs, which have modifiable firmware, can be vulnerable to these attacks. Practically, the firmware modification attacks can be carried out by injecting the malware into the target embedded PLCs [22].
In the testbed, the ControlLogix back-plane has firmware so that the device provides communication with other controllers as well as I/O modules. By modifying the ControlLogix firmware, malware could be created. As result of malware injection into the testbed controllers, significant system disruptions and motor or controller failures can be seen.

D. Attacks on HMI and Programming Stations

The critical infrastructures can be hijacked effectively by injecting malware on HMI computers or programming station computers. Many SCADA computers do not have any effective anti-virus protection. Even if anti-virus programs are installed on the computers, they are vulnerable to cyber-attacks because these computers’ update cycles are extremely long. Thus, it is possible that the control process network can be vulnerable to malware injections.

Process network malware injection: The process network malware can infiltrate through the external network or internal network. While on the internal network the injection could be achieved by removable storage devices (such as CDs, DVDs, floppy disks, as well as USB drives). Network-based attack techniques might be carried out on the external network. As an example, for network-based attack the Sandworm was carried to hack Cimplicity HMI Solution Suite by researchers [23]. The results show that by using such malware, the HMI or programming computer could be used to manipulate actual SCADA data or network.

Our cyber-physical testbed enables us to see the consequences of process network malware. If the malware is injected in the programmer or HMI computer, high-impact results are observed because these computers are thought of as the main workstation of the testbed. By implementing malware to the programming station or HMI computer, the attacker can directly affect the power generation units and consequently the functionality of the testbed totally could change.

VI. CONCLUSIONS

In this work, a cyber-physical testbed based on power generation is explained. Two different power generation units are used with two different design approaches; first, blower motors are connected to each others and second an AC motor is directly coupled to a permanent magnet DC motor. Power generation units are controlled with IP based real-time intelligent electronic devices, in this way the system transformed into a cyber-physical system. We separately discuss intelligent electronic devices and their connection (controllers, HMI devices, drives, and network components) on the testbed.

Furthermore, the testbed is structured to gather static and dynamic information available. Data collection on the testbed has demonstrated that static data is usually seen in a human readable format, while dynamic data is acquired in a computer readable format.

Based on the data gathering process, the testbed architecture is evaluated in terms of the probability and availability of likelihood cyber-attacks on the SCADA systems. Proposed experiments in this paper demonstrate that the testbed is an effective tool to expose cyber-attacks that may cause massive amounts of damage to the system and enables us to study them.

ACKNOWLEDGMENT

The authors would like to thank the Office of Naval Research (ONR) for their support under the award number 15114581.

REFERENCES