# REPORT DOCUMENTATION PAGE

Form Approved OMB NO. 0704-0188



| 1. REPORT DATE (DD-MM-YYYY) | 2. REPORT TYPE | 3. DATES COVERED (From - To) |
|---|---|---|
| 26-01-2017 | Final Report | 15-Aug-2015 - 14-Aug-2016 |

**4. TITLE AND SUBTITLE**
Final Report: SCADA Testbed for Security and Forensics Research

**5a. CONTRACT NUMBER**
W911NF-15-1-0506

**5b. GRANT NUMBER**

**5c. PROGRAM ELEMENT NUMBER**
611103

**6. AUTHORS**
Irfan Ahmed, Vassil Roussev, Golden G. Richard III

**5d. PROJECT NUMBER**

**5e. TASK NUMBER**

**5f. WORK UNIT NUMBER**

**7. PERFORMING ORGANIZATION NAMES AND ADDRESSES**
University of New Orleans
2000 Lakeshore Drive
1005 Administration Bldg
New Orleans, LA 70148 -0001

**8. PERFORMING ORGANIZATION REPORT NUMBER**

**9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS (ES)**
U.S. Army Research Office
P.O. Box 12211
Research Triangle Park, NC 27709-2211

**10. SPONSOR/MONITOR'S ACRONYM(S)**
ARO

**11. SPONSOR/MONITOR'S REPORT NUMBER(S)**
66841-CS-RIP.1

**12. DISTRIBUTION AVAILIBILITY STATEMENT**
Approved for Public Release; Distribution Unlimited

**13. SUPPLEMENTARY NOTES**
The views, opinions and/or findings contained in this report are those of the author(s) and should not contrued as an official Department of the Army position, policy or decision, unless so designated by other documentation.

**14. ABSTRACT**
This report presents a supervisory control and data acquisition (SCADA) testbed recently built at the University of New Orleans. The testbed consists of models of three industrial physical processes: a gas pipeline, a power transmission and distribution system, and a wastewater treatment plant–these systems are functional and implemented at small-scale. It utilizes real-world industrial equipment such as transformers, programmable logic controllers (PLC), aerators, etc., bringing it closer to modeling real-world SCADA systems. Sensors, actuators, and PLCs are deployed at each physical process system for local control and monitoring, and the PLCs are also

**15. SUBJECT TERMS**
SCADA, Control System, PLC, HMI, Gas Pipeline, Wastewater Treatment, Power Distribution, Power Grid

| 16. SECURITY CLASSIFICATION OF: | | | 17. LIMITATION OF ABSTRACT | 15. NUMBER OF PAGES | 19a. NAME OF RESPONSIBLE PERSON |
|---|---|---|---|---|---|
| a. REPORT | b. ABSTRACT | c. THIS PAGE | | | Irfan Ahmed |
| UU | UU | UU | UU | | 19b. TELEPHONE NUMBER: 504-280-4409 |

**Report Title**

Final Report: SCADA Testbed for Security and Forensics Research

**ABSTRACT**

This report presents a supervisory control and data acquisition (SCADA) testbed recently built at the University of New Orleans. The testbed consists of models of three industrial physical processes: a gas pipeline, a power transmission and distribution system, and a wastewater treatment plant–these systems are functional and implemented at small-scale. It utilizes real-world industrial equipment such as transformers, programmable logic controllers (PLC), aerators, etc., bringing it closer to modeling real-world SCADA systems. Sensors, actuators, and PLCs are deployed at each physical process system for local control and monitoring, and the PLCs are also connected to a computer running human-machine interface (HMI) software for monitoring the status of the physical processes. The testbed is a useful resource for cybersecurity research, forensic research, and research-related education on different aspects of SCADA systems such as PLC programming, protocol analysis, and demonstration of cyber attacks.

---

## Enter List of papers submitted or published that acknowledge ARO support from the start of the project to the date of this printing. List the papers, including journal references, in the following categories:

### (a) Papers published in peer-reviewed journals (N/A for none)

Received Paper

**TOTAL:**

**Number of Papers published in peer-reviewed journals:**

---

### (b) Papers published in non-peer-reviewed journals (N/A for none)

Received Paper

**TOTAL:**

**Number of Papers published in non peer-reviewed journals:**

---

### (c) Presentations

**Number of Presentations:** 0.00

## Non Peer-Reviewed Conference Proceeding publications (other than abstracts):

Received Paper

**TOTAL:**

**Number of Non Peer-Reviewed Conference Proceeding publications (other than abstracts):**

## Peer-Reviewed Conference Proceeding publications (other than abstracts):

Received Paper

**TOTAL:**

**Number of Peer-Reviewed Conference Proceeding publications (other than abstracts):**

## (d) Manuscripts

Received Paper

**TOTAL:**

**Number of Manuscripts:**

## Books

Received Book

**TOTAL:**

| Received | Book Chapter |
|---|---|

**TOTAL:**

## Patents Submitted

## Patents Awarded

## Awards

### Graduate Students

| NAME | PERCENT_SUPPORTED |
|---|---|

**FTE Equivalent:**
**Total Number:**

### Names of Post Doctorates

| NAME | PERCENT_SUPPORTED |
|---|---|

**FTE Equivalent:**
**Total Number:**

### Names of Faculty Supported

| NAME | PERCENT_SUPPORTED |
|---|---|

**FTE Equivalent:**
**Total Number:**

### Names of Under Graduate students supported

| NAME | PERCENT_SUPPORTED |
|---|---|

**FTE Equivalent:**
**Total Number:**

## Student Metrics

This section only applies to graduating undergraduates supported by this agreement in this reporting period

The number of undergraduates funded by this agreement who graduated during this period: ..... 0.00

The number of undergraduates funded by this agreement who graduated during this period with a degree in science, mathematics, engineering, or technology fields:..... 0.00

The number of undergraduates funded by your agreement who graduated during this period and will continue to pursue a graduate or Ph.D. degree in science, mathematics, engineering, or technology fields:..... 0.00

Number of graduating undergraduates who achieved a 3.5 GPA to 4.0 (4.0 max scale):..... 0.00

Number of graduating undergraduates funded by a DoD funded Center of Excellence grant for Education, Research and Engineering:..... 0.00

The number of undergraduates funded by your agreement who graduated during this period and intend to work for the Department of Defense ..... 0.00

The number of undergraduates funded by your agreement who graduated during this period and will receive scholarships or fellowships for further studies in science, mathematics, engineering or technology fields: ..... 0.00

## Names of Personnel receiving masters degrees

NAME

**Total Number:**

## Names of personnel receiving PHDs

NAME

**Total Number:**

## Names of other research staff

| NAME | PERCENT_SUPPORTED |
|---|---|

**FTE Equivalent:**

**Total Number:**

## Sub Contractors (DD882)

## Inventions (DD882)

## Scientific Progress

## Technology Transfer

# SCADA TESTBED FOR SECURITY AND FORENSICS RESEARCH

FINAL TECHNICAL REPORT

submitted to

*Army Research Office*

by

*Irfan Ahmed*

DEPARTMENT OF COMPUTER SCIENCE
UNIVERSITY OF NEW ORLEANS

January 26, 2017

# Contents

# List of Figures



# List of Tables

# SCADA Testbed for Security and Forensics Research

**Abstract**

This report presents a supervisory control and data acquisition (SCADA) testbed recently built at the University of New Orleans. The testbed consists of models of three industrial physical processes: a gas pipeline, a power transmission and distribution system, and a wastewater treatment plant–these systems are fully-functional and implemented at small-scale. It utilizes real-world industrial equipment such as transformers, programmable logic controllers (PLC), aerators, etc., bringing it closer to modeling real-world SCADA systems. Sensors, actuators, and PLCs are deployed at each physical process system for local control and monitoring, and the PLCs are also connected to a computer running human-machine interface (HMI) software for monitoring the status of the physical processes. The testbed is a useful resource for cybersecurity research, forensic research, and education on different aspects of SCADA systems such as PLC programming, protocol analysis, and demonstration of cyber attacks.

## 1 Introduction

Supervisory control and data acquisition (SCADA) systems are an integral and critical part of industrial automation. They are classified as cyber physical systems, and are used to monitor and control industrial and infrastructural physical processes such as electricity distribution, water and waste management, and gas pipelines.

Early SCADA systems were designed to run as isolated networks that did not require any specific cybersecurity mechanisms. They consisted of simple input/output devices transmitting the signals between master devices and remote terminal units. In recent years, SCADA systems have evolved to communicate over public IP networks, making them vulnerable to cyber-attacks [17],[13].

The integration of SCADA systems within a much wider network brings threats that were unimagined at the time these systems were conceived. Stuxnet, for instance, is a malware discovered in June 2010 specifically written to target industrial automation systems, and has infected around 50,000 to 100,000 computers worldwide [11]. The existence of Stuxnet provides sufficient evidence to realize the severity of the security issues in SCADA system and demands immediate attention from cyber security and forensic research communities to address these issues.

**Problem Statement.** Research on SCADA systems is challenging [9]. These systems have the critical requirement of high availability, use resource constrained computing devices, and typically run legacy operating system software and protocols. If they malfunction or are attacked, the impact on the physical world can be catastrophic, including potential loss of human life and severe damage to the environment. Thus, to perform effective applied research with real-world significance, it is imperative to build realistic SCADA systems for development and testing.

**SCADA Testbed.** This report presents a laboratory-scale SCADA testbed recently built at the University of New Orleans, which is designed to closely represent real-world SCADA systems. It employs equipment deployed in real industrial settings, such as programmable logic controllers (PLC), transformers, aerators, and an air compressor, and utilizes popular SCADA protocols for communication such as Modbus [7], EtherNet/IP [6] and PROFINET [5].

The testbed models three physical processes: a gas pipeline, a power distribution system, and a wastewater treatment system. These systems use functional physical models and perform operations

such as gas compression, voltage transformations, and water aeration. The physical processes are controlled by PLCs and monitored through local human machine interface (HMI) software.

The gas pipeline controller maintains the specified pressure of gas (modeled with compressed air) flowing through the pipes. If the pressure increases beyond a predefined threshold, the controller releases the gas to reduce the pressure. The power transmission and distribution system consists of four grid stations representing voltage transformers. The controller for the power distribution system ensures the steady supply of electricity to grid stations. If the power supply to a station is blocked (i.e., a relay is powered off), the controller automatically enables backup generators (additional sources of wall power in our simulation). The wastewater treatment system filters out impurities in wastewater. It consists of a sequence of steps including sedimentation, aeration, and clarification–the water in the system feeds through a tank for each of these processes in sequence. If the level of water in the initial tank is determined to be too high, the system is designed to automatically shut off the flow of water.

The rest of the report is organized as follows: Section §2 presents an overview of the testbed, followed by the implementation details of the physical processes in section §3. Sections §4 and §5 cover the usage and limitations of the testbed. Section §6 presents the related work followed by a conclusion in section §7

## 2 Overview of the Testbed

Figure 1 illustrates the design and components of the testbed. The testbed has two major sections: one is the control center containing the HMI and data historian, and the other is the remote site where the SCADA components such as sensors, actuators, and PLCs are installed to directly monitor and control a physical process such as power distribution, wastewater treatment, or a pipeline. The SCADA components are interconnected using PLCs and Ethernet switches. Each PLC uses a SCADA protocol to communicate with the HMI, sending data representing the current state of its physical process as well as relaying data representing operator inputs. The HMI receives the data and presents a graphical representation of system state to a control operator.

The testbed includes PLCs manufactured by Allen-Bradley, Schneider Electric, and Siemens. They support the Modbus, EtherNet/IP, and PROFINET protocols. The PLC data in the power distribution system includes the voltage from the substation transformers as well as whether power is provided to each subsection of the system. In the gas pipeline, PLC data includes the gas pressure in the pipeline as well as whether the solenoid valve is set to release gas. In the wastewater treatment plant, the PLC data includes the water level in the initial tank and whether the pump is currently running.

## 3 Implementation Details

In reality, a large SCADA system is spread over a wide area and is not feasible economically to mimic exactly as a testbed. Instead, each remote site is simulated and installed in a 24"H×24"W×8"D movable trolley. The scaled physical process is installed at the top of the trolley, and below is a cabinet where the PLCs and other equipment–such as an Ethernet switch, protocol converter, power supply, transformer, and aerato–are installed. The proposed setup is space efficient and also

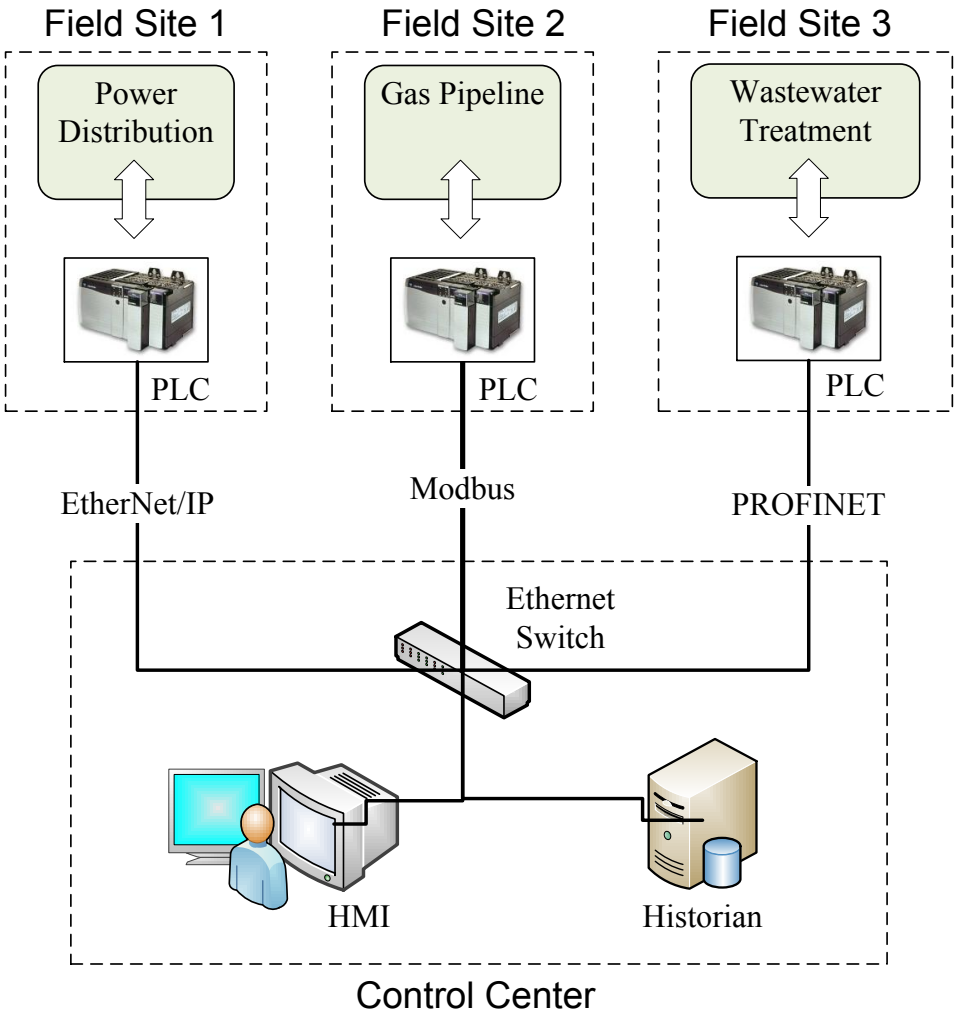


Figure 1: Overview of the testbed of SCADA system

provides convenient mobility of the testbed to classrooms, conference centers and other places. The cabinet also provides physical protection to embedded devices. This section further provides the implementation details of each physical process and its interaction with cyber.

## 3.1 Gas pipeline

Gas pipelines are a popular way to transfer large volume of compressed gas across hundreds of kilometers. Controllers are deployed across the pipeline to maintain the gas pressure to avoid any damage to the pipeline. The testbed simulates a gas pipeline (refer to Figures 2 and 3) utilizing compressed air. The pipe is fed with an air compressor. The other end of the pipe is closed, but contains a release valve controlled by a solenoid (which is normally off). When the compressor is turned on, it compresses the air and transfers it from one side of the pipe to the other. The pressure in the pipe is managed by a PLC, which will temporarily release the compressed air from the valve when the pressure exceeds a chosen threshold. When a lower pressure threshold is reached, the PLC will close the solenoid, and the pressure begins to increase again.

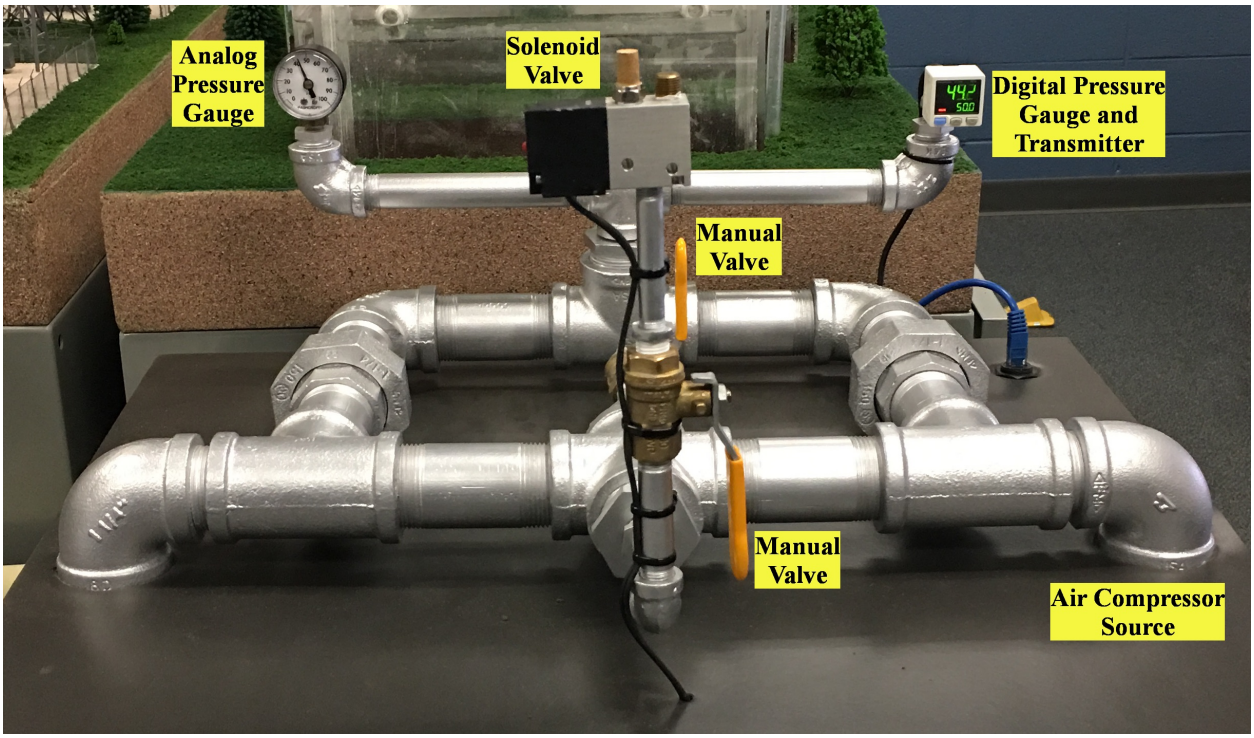


Figure 2: Top-view of the gas pipeline simulator

The testbed has two manual valves. One is normally open and located in-line between the pipeline and the solenoid valve. The other is normally closed and located in-line to an always-open exhaust–if this is opened, the system will not be able to remain pressurized. If both valves are closed, the system will not be able to relieve pressure; however, the system is built such that this would simply overwhelm the system's air compressor.

**Physical System Layout.** The pipeline is built with galvanized steel piping. The air compressor is designed to provide a maximum pressure of 120 PSI. From the air compressor, the core piping is designed as a square loop with two corners as 90 degree couplings and two others as t-shaped couplings. One of the t-shaped couplings is sealed, and the other is used to receive exhaust from the air pump.

Extending as a quad-coupling from one side of the loop are two exhausts, one on each open end of the coupling. One of these is attached to a manual relief valve with no electrical control–this valve is normally closed and will immediately vent if opened. The other open end of the coupling is attached to a normally-open manual relief valve which is then attached in-line to a solenoid valve that is normally closed. If the manual valve on this side of the coupling is closed, the control system will be unable to automatically vent as needed, as the pressurized air will be cut off before the solenoid valve.

Extending from a t-coupling attached in-line on the other side of the primary loop is an additional t-coupling–one end is attached to a mechanical pressure gauge that measures 0-100 PSI, and the other end is a pressure gauge/transmitter (Panasonic DP-102A-N-P) that connects to an analog input on a Schneider Electric PLC analog slot module (Schneider TM3AM6) as well as a discrete input on the Schneider Electric PLC main module (Schneider TM221CE16R). (Table 1 summarizes the


Figure 3: Cabinet-view of the gas pipeline simulator

components of pipeline simulator.)

**Cyber-Physical Interactions.** The primary interactions done through cyber-physical control sys-

```
void system_loop(){
   if (is_enabled(system_run))
     enable(pump_on)
   else
     enable(air_bleed_timer)
}
void pump_on_loop(){
   if (is_enabled(pump_on))
     enable(air_pump_run)
     if ((pressure_signal > HMI_pressure_HI) ||
        (solenoid_on && pressure_signal > HMI_pressure_LO))
        enable(solenoid_on)
 }
void solenoid_loop(){
   if (is_enabled(solenoid_on) ||
       is_enabled(air_bleed_timer) ||
     is_enabled(manual_force_on))
       enable(solenoid_on)
 }
```

Listing 1: PLC logic (pseudocode) of pipeline simulator

Table 1: The components of the pipeline simulator

| Manufacturer | Component ID | Component Type | Component Description |
|---|---|---|---|
| Grainger | P251SS-024-D | Solenoid Valve | Used to relieve pressure; 24VDC for control |
| Panasonic | DP-102A-N-P | Pressure Gauge/Transmitter | 0.6-5VDC output, 0-145PSI measurements |
| Phoenix | 29 66 17 1 | Terminal Block Relay | 24VDC, SPDT |
| Schneider | TM221CE16R | PLC Processing Unit | Modicon M221, 100-240VAC, 9 discrete inputs, 7 relay outputs |
| Schneider | TM3AM6 | PLC Analog I/O Card | 4 inputs, 2 outputs |
| Siemens | 5SY4 111-7 | Circuit Breaker | 1 pole, 15 amp, C curve |
| Siemens | 5SY4 118-7 | Circuit Breaker | 1 pole, 5 amp, C curve |
| Siemens | 6EP1 332-5BA10 | Power Supply | 120/230VAC, 24VDC, 4A |

tems are pressure measurements as well as solenoid access for the relief valve and air compressor– these are directly connected with the I/O modules of the Schneider Electric PLC. A ladder logic program (refer to listing 1 for pseudocode) is installed in the PLC, which uses pressure readings to temporary release the gas from the valve for maintaining the gas pressure in the pipeline.

When the PLC begins to run, it executes the ladder logic. On the first scan, predefined minimum and maximum pressure values are set, and a five-second timer for bleeding air is also initialized. If at any time the compressor pressurizes the system beyond the set maximum, the solenoid valve will activate. The air pump and solenoid valve are controlled by the PLC through two relays: one is activated upon an air pump run command; and the other is activated upon a solenoid open command. These are controlled through discrete outputs on the PLC's main module.

The PLC is also connected with HMI (through an Ethernet switch), sending the current state of the pipeline including the gas pressure, valve and compressor status (on/off) to HMI. The HMI also receives commands to change the maximum and minimum set points, as well as to turn the compressor on and off.

## 3.2 Power transmission and distribution

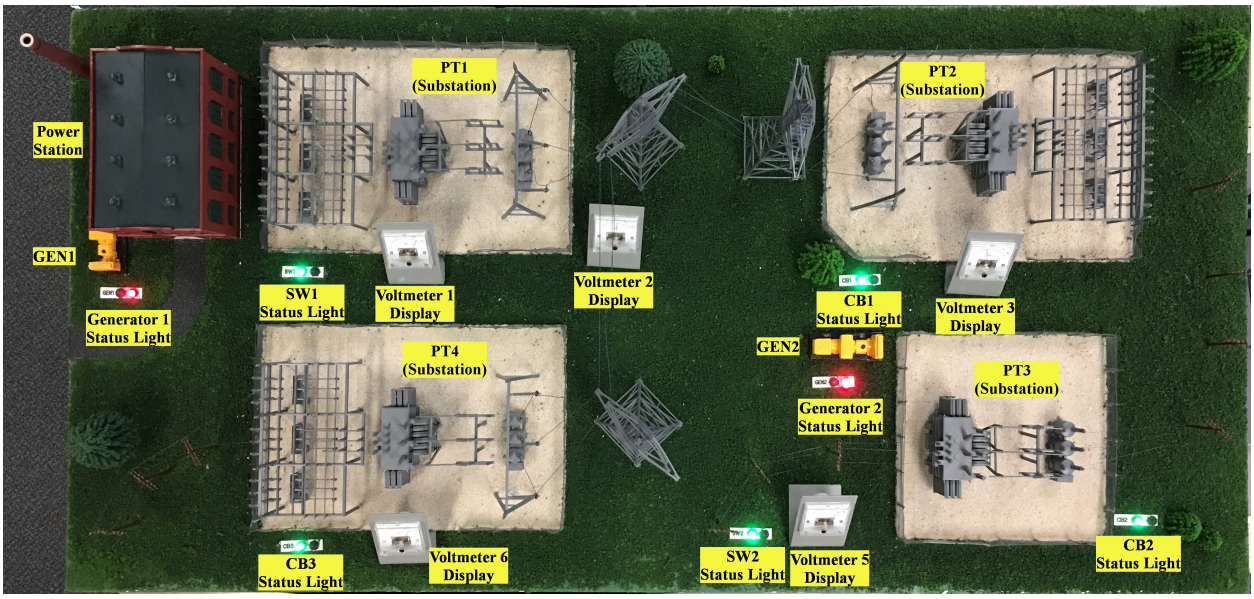


Figure 4: Top-view of the power transmission and distribution simulator

Figure 5: Cabinet-view of the power transmission and distribution simulator

```
void gen1_loop() {
  if (switched_off(SW1) &&
      is_disabled(GEN1)) {
    sleep(5);
```

```
    enable(GEN1);
  }
  else if (switched_off(SW1) &&
     is_enabled(GEN1))
    continue;
  else
    disable(GEN1);
}
void gen2_loop() {
  if ((switched_off(CB1) ||
       switched_off(SW2) ||
       switched_off(CB2)) &&
      is_disabled(GEN2)) {
    sleep(5);
    enable(GEN2);
  }
  else if ((switched_off(CB1) ||
      switched_off(SW2) ||
      switched_off(CB2)) &&
     is_enabled(GEN2))
    continue;
  else
    disable(GEN2);
}
```

Listing 2: PLC logic (pseudocode) of power transmission and distribution simulator

The power transmission and distribution system carries electricity from power generation sources through transmission lines and substations finally to individual consumer. In the testbed, the simulated power transmission and distribution system (refer to Figures 4 and 5)is built to transmit power (120VAC from the wall) through a set of substations (simulated with transformers) and ultimately onward elsewhere through two points of transfer. It is designed to handle failures of a number of components (simulated through software switches in an HMI that interact with relays and can be arbitrarily turned off) through the presence of two simulated generators (also 120VAC from the wall).

Throughout the circuit, transformers are used to modify the voltage of power running through the substations and beyond. As the power generation is simply 120VAC from the wall, the first generator supplies power before the first transformation, and the second generator provides power to an area of the circuit after a 30VAC to 120VAC transformation.

Along the route, voltage measurements are taken; however, these are not used to modify the status of the generators. Instead, five seconds after the appropriate switches are turned off (and thus the corresponding relays are opened), the simulated generators are programmed to then switch on. They will run indefinitely until the appropriate switches are returned to the on state. The PLC ladder logic is programmed generally relative to the two generators and there is only one PLC used for this portion of the testbed. The only network communication on the system is done to and from the HMI; communication between the PLC and the power simulation is facilitates electricity measurement and relay signaling.

**Electrical Layout of the System.** Figure 6 illustrates the electrical layout of the power transmission and distribution system. The simulation consists of a power house and four substations, as well

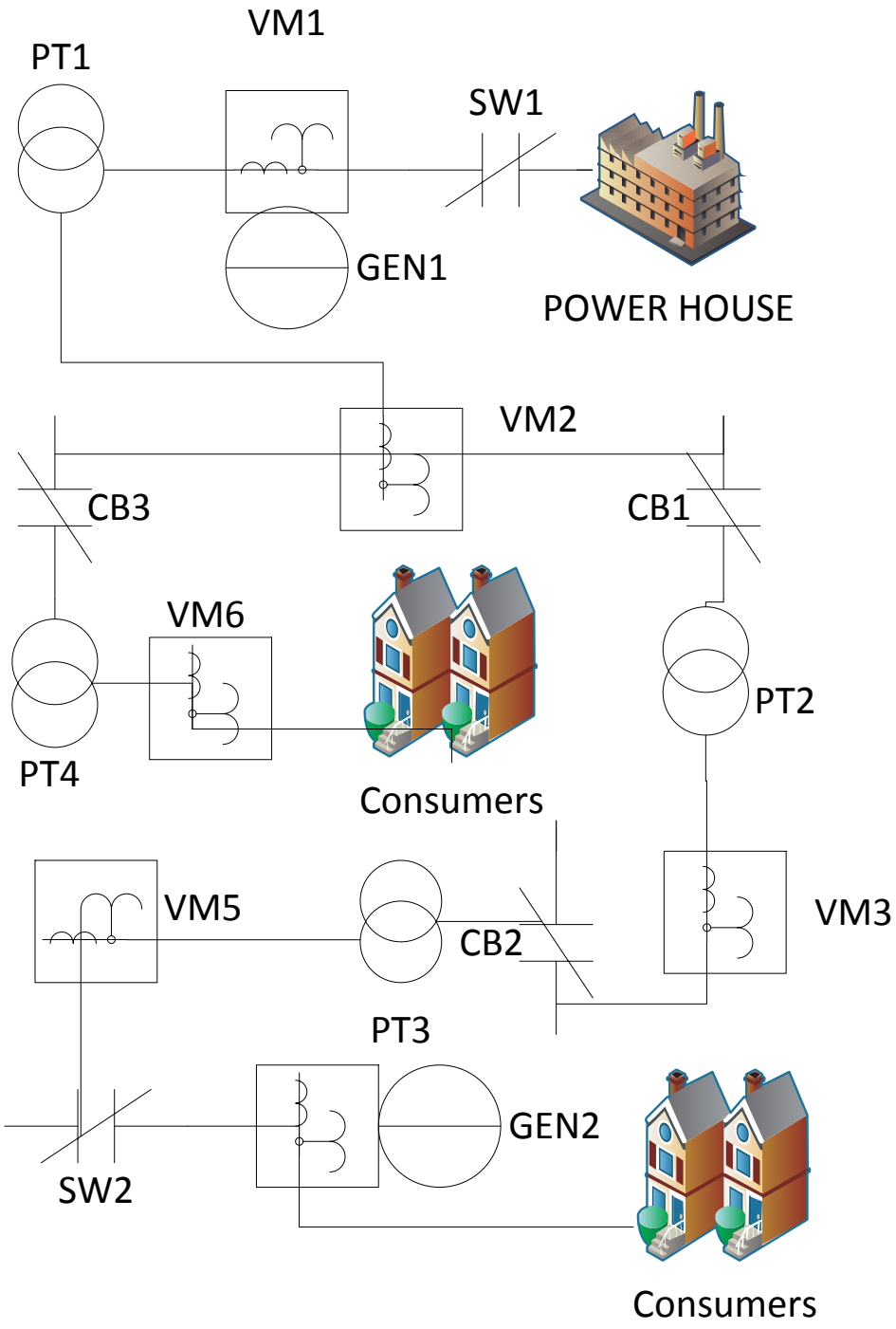


Figure 6: Schematic diagram of the power transmission and distribution simulator

as two lines that abstractly would continue to other areas. Electrically, the source comes from the wall, through a breaker on one of the wires, then to the generators and then to the rest of the system. Along this same line, the circuit then proceeds through the first relay marked SW1. Then 120VAC generator (GEN1) power is connected to the circuit, and there is a transducer (VM1) that creates a current signal of 4-20mA of 24VDC power, which is sent through an ammeter (AM1) and then

Table 2: The components of the power transmission and distribution simulator

| Manufacturer | Component ID | Component Type | Component Description |
|---|---|---|---|
| AcuAMP | VACT150-42L | AC Voltage Transducer | Converts 0-150VAC input to 4-20mA output. Transducers convert one form of energy to another. |
| Allen-Bradley | 1769-IF8 | CompactLogix Analog Input Module | PLC slot module for analog inputs; 8 differential or single-ended inputs; voltage range is $\pm$10VDC |
| Allen-Bradley | 1769-IQ16 | CompactLogix Digital Input Module | PLC slot module for digital inputs; 16 point, sink or source, provides 24VDC power |
| Allen-Bradley | 1769-L30ER | CompactLogix PLC CPU Unit | PLC controller; has 1 USB and 2 Ethernet port connections |
| Allen-Bradley | 1769-OW8I | CompactLogix Relay Output | PLC slot module for relay outputs; AC/DC relay contact module; 8 normally-open outputs; AC voltage range 5-265V, 5-125VDC |
| Allen-Bradley | 1769-PA4 | CompactLogix PLC Power Supply | 120/240VAC input, 24VDC output |
| Finder | 62.33.9.024.0070 | Relay | Relay with 250VAC contact voltage, 24VDC coil voltage, 3PDT; relays are electromagnetic switches |
| Hammond Power Solutions | PH50MQMJ | Isolation Transformer | 480x240 VAC Primary, 240x120 VAC Secondary; used to manage voltages provided to particular subsections of the circuit. |
| Siemens | 5SY4 111-7 | Circuit Breaker | 1 pole, 5 amp, C curve; circuit breakers are designed to trip upon overcurrent. |
| Siemens | 5SY4 118-7 | Circuit Breaker | 1 pole, 15 amp, C curve; see above breaker for description. |
| Siemens | 6EP1 332-5BA10 | DC Power Supply | Supplies 24VDC from 85-264VAC source |
| Siemens | 6GK52080BA10-2AA3 | Ethernet Switch | 8-port managed Ethernet switch; used for IP connectivity between testbed devices as well as outside |
| Square D | | Ground Bar | 7 position ground bar; used to connect components to ground |
| Weidmuller | 1020100000 WDU4 | Terminal Block | Used to arrange wire connections between various components |

to an input on the analog input module (331PLC). At this point, the AC circuit passes through a transformer (PT1), which steps from 120VAC to 60VAC. Following the power transform, a second transducer (VM2) is attached which takes power from the circuit, changing it to a 4-20mA signal, which is sent through another ammeter (AM2) and then to an analog input on 331PLC.

At this point, a branch occurs. First on the branch is a relay (CB3). Then the branch circuit proceeds through a transformer (PT4) converting 60VAC to 120VAC. Then is another transducer (VM6), which connects to an ammeter (AM6) and then to an analog input on (331PLC). The rest of the branch is abstracted away, assumed to continue outward to consumers.

Continuing along the main line past the branch, there is a relay (CB1). Then the circuit proceeds through a 60VAC to 30VAC transformer (PT2). Another transducer (VM3) sends a 4-20mA DC signal through an ammeter (AM3), then to an analog input on 331PLC. Continuing the AC circuit, there is a relay (CB2), and then a power transformer (PT3), converting 30VAC to 120VAC. Following this is another transducer (VM4) which is directly connected to a 331PLC analog input.

Further along the AC circuit, there is a relay (SW2), and then the second 120VAC generator is attached. At this point, there is a transducer (VM5) to ammeter (AM5) combination attached to a 331PLC input. The system here is abstracted away again, assumed to continue to consumers. (Table 2 summarizes the components of the simulator.)

**Cyber-Physical Interactions.** Interactions with the PLC are performed through analog inputs on 331PLC (connected with transducer and ammeter) as well as through relay manipulation. The PLC itself is able to monitor voltage by multiplying the current on the analog inputs by known resistances of each input.

However, the primary logic of this system (refer to listing 2 for pseudocode) is performed relative to the status of the software switches that are intended to be accessed through the HMI. The status of these switches are all represented as data objects. There are four switches that are used to determine

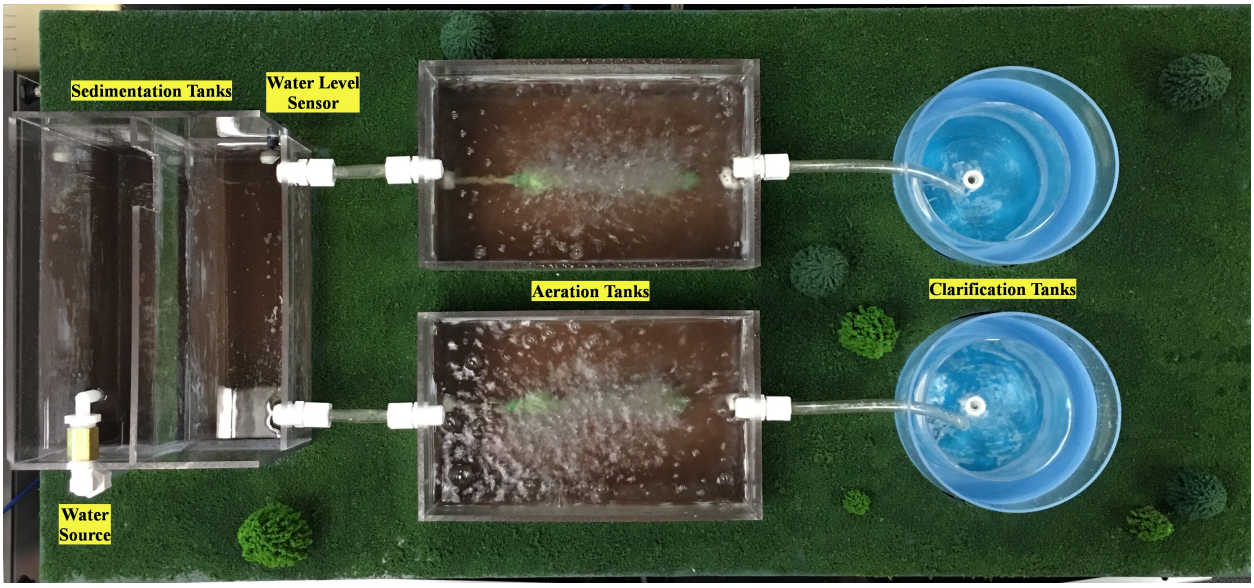


Figure 7: Top-view of the wastewater treatment simulator

the states of the generators.

The status of generator 1 is determined by one switch i.e. SW1 (aside from a master switch–the master switch must be turned on for the logic to proceed). If the relevant digital input Boolean is turned on, an internal Boolean will be turned on and checked when the PLC needs to check switch status. In the generator 1 control logic, if this internal status Boolean is switched off (as well as the master switch), a 5 second timer will begin. When the timer completes, generator 1's relay will be activated and the generator will be turned on indefinitely until both the master switch and switch 1 are turned back on.

The status of generator 2 is determined in much the same way; however, its status is determined by the state of the master switch as well as SW2, CB1, and CB2. If any of these are switched off, a second five-second timer is triggered, after which the generator 2 relay will be turned on indefinitely until all three power switches and the master switch are turned back on.

## 3.3 Wastewater treatment

Wastewater is generally referred to as the water that is no longer suitable for its current use. The treatment process converts it into an effluent to either dispose it off or repurpose for some other use. In the testbed, a wastewater treatment plant is simulated (refer to Figures 7 and 8), including the treatment processes of sedimentation, aeration and clarification. The setup consists of three sets of tanks lined up in a sequence, a water pump to push water from one tank to other, a PLC to monitor the water level of a tank to avoid overflowing, and HMI for remote monitoring and control.

When the system is switched on, the wastewater is pumped from the storage tank into the sedimentation tank consisting of two levels. The water flows from one level to the other and the solid particles sediment in these tanks. In the second sedimentation tank, the water without those solid impurities flows through two pipes to two different aeration tanks. Each aeration tank has its own air diffuser to aerate the water and impurities are further cleaned. These diffusers can be controlled through HMI. After the aeration process, the water flows through small pipes from the

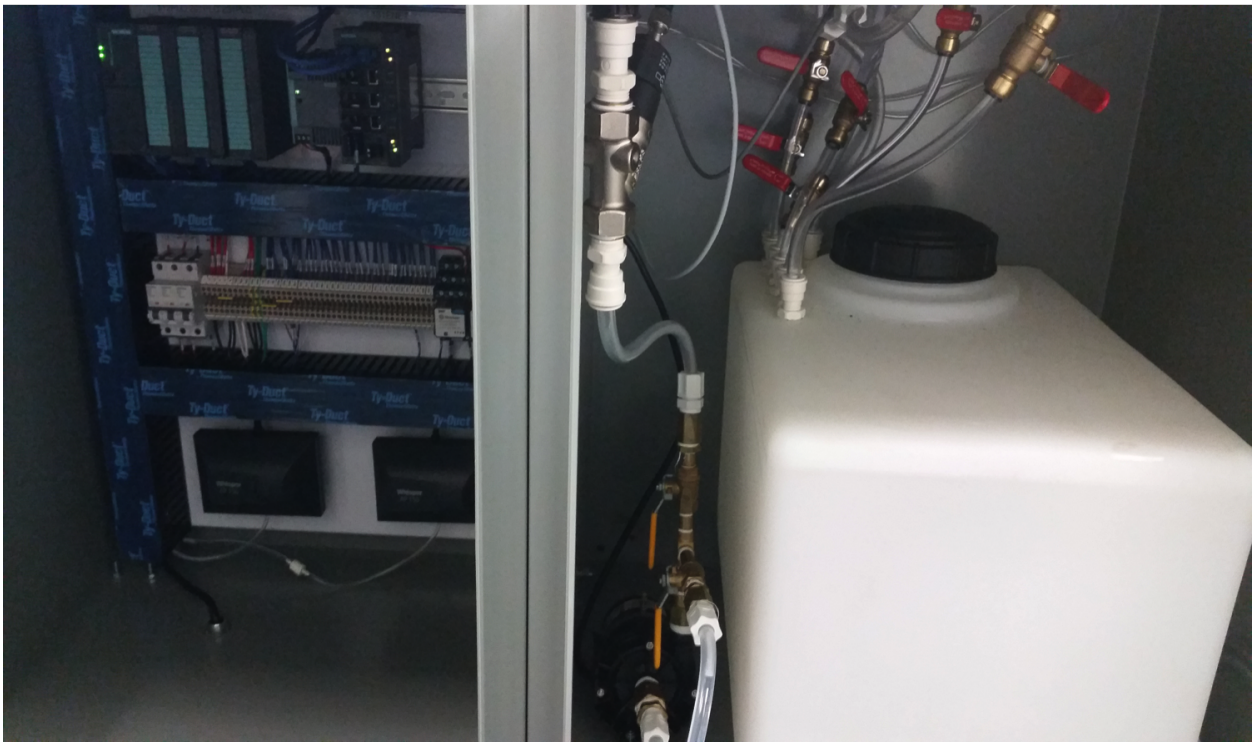

Figure 8: Cabinet-view of the wastewater treatment simulator

two aeration tanks to two clarifier tanks. Once the clarification process is complete, the water is returned to the storage tank to recycle. Throughout the entire process, the water level is monitored in the sedimentation tank using an optical liquid level switch to prevent overflow.

**Physical Layout of the Simulator.** The simulation consists of a water pump and four different tanks. A quiet water pump (120VAC, 0.52Amp) is used to push water from the main storage tank to the sedimentation tank. The main storage tank (Den Hartog SP0016-MM) has vented lids and can store 16 gallons of water. The remaining three water tanks are built with acrylic transparent sheets cut to size and pasted using 16-gauge hypo applicator. Acrylic circles are used in the clarification bed, and acrylic cement to seal the tanks to avoid water leakage.

Four manual valves are used to control the flow of water to tanks. Two of them control the inlet of water into the storage tank. One of them is located at the pipe between pump and sedimentation tank to control the water flow pushed by the pump to the tank. Another valve is installed on a pipe to empty the main storage tank. One end of the pipe is attached to the tank and the other is open to allow drainage from the system if necessary. Furthermore, six valves are used to control the outlet of water from tanks: two with the sedimentation tank covering both levels, two with aerators, and two with the tank for clarification.

Furthermore, a Whisper aquarium air pump (Tetra 26075) is used to pump air to the aeration tanks. Air diffusers (Jardin A11010600UX0515) are kept inside each aeration tank to diffuse the air. In the sedimentation tank, there is an optical liquid level switch (Madison OPT-4306-5) attached to the tank wall to monitor the liquid level. The water pump status and air diffuser status are both controlled by a Siemens PLC (S7-300) through three relays. (Table 3 summarizes the components of the simulator.)

Table 3: The components of the wastewater treatment simulator

| Manufacturer | Component ID | Component Type | Component Description |
|---|---|---|---|
| Siemens | 5SY4 118-7 | Circuit Breaker | 1 Pole, 15 Amp, C Curve |
| Siemens | 5SY4 111-7 | Circuit Breaker | 1 Pole, 5 Amp, C Curve |
| Siemens | 6EP1 332-5BA10 | Power Supply | 120/130VAC-24VDC, 4A |
| Siemens | 6ES7 315-2EH14-0AB0 | CPU | Simatic CPU 315-2 PN/DP, Profinet and Profibus |
| Siemens | 6ES7 953-8LL31-0AA0 | Memory Module | S7-300 SD Memory Module |
| Siemens | 6ES7 321-1BH02-0AA0 | Digital Input Module | 24VDC, 16PT |
| Siemens | 6ES7 322-1BF01-0AA0 | Digital Output Module | 24VDC, 8 PT |
| Siemens | 6GK52080BA102AA3 | Ethernet Switch | 8 Port Managed |
| Finder | 62.33.9.024.0070 | Relay | Relay with 250VAC contact voltage, 24VDC coil voltage, 3PDT; relays are electromagnetic switches that are designed to be controlled with an electric signal. |
| Square D | | Ground Bar | 7 position ground bar; used to connect components to ground |
| Weidmuller | 1020100000 WDU4 | Terminal Block | Used to arrange wires |

```
void waterpump_on() {
   if (switched_on(system) &&
       is_disabled(high_level_switch))
       enable(water_pump)
}
void aerator1_on(){
   if (switched_on(system) &&
       is_enabled(aerator_1_select))
       enable(aerator_1)
}
void aerator2_on(){
   if (switched_on(system) &&
       is_enabled(aerator_2_select))
       enable(aerator_2)
 }
```

Listing 3: PLC logic (pseudocode) of Wastewater treatment simulator

**Cyber-Physical Interactions.** The main cyber-physical interaction in this setup is to control the water pump and the aerators. Switches are set up in the HMI, which is used to activate the program logic to control the water pump and aerators. When the main switch is turned on, the water pump starts and pushes water to sedimentation tank. The controller observes the liquid level of the tank, and turns off the pump and aerators when the level of water exceeds a certain threshold. Listing 3 presents the pseudocode.

The HMI has a three-way switch to control the aerators. The three modes of this switch allow an operator to turn either or both of the aerators on. The HMI also provides a switch to turn the pump off.

# 4 Enhancements to SCADA Research and Pedagogy

This section discusses the benefits of the testbed for research and pedagogy.

## 4.1 Research

In particular, the testbed is suitable for cybersecurity and forensic research because it represents a real-world SCADA system by utilizing industrial equipment and simulating functional physical processes. For instance, the current efforts (of utilizing the testbed) include the analysis of Allen-Bradley's PCCC protocol for surveying potential cyber attacks, extracting program logic from network traffic capture, and identifying anomalies in the network traffic of the protocol.

**Cyber attacks and Vulnerabilities.** Vectors for cyber-attacks of the testbed and similar SCADA systems in industry are likely to be related. For instance, a vulnerability found in a protocol used by the testbed can also affect the systems in the industry using the same protocol.

**Research Prototype Evaluation.** The testbed has the potential to deliver convincing evaluation results of cybersecurity solutions because it enforces the constraints of a typical SCADA system in the evaluation process–including the 24/7 availability requirement of SCADA services, resource-constrained embedded devices, interaction of cyber and physical worlds, and the use of communication protocols exclusively used in SCADA systems.

**Digital Forensics.** The testbed enables digital forensic research on SCADA systems because the development of forensic tools and techniques requires deep analysis of these systems for extracting, understanding, and analyzing data including firmware, and program logic (written in adder-logic, instruction-list etc.) in PLCs, network traffic, and HMI, historian and other services running in a control center. The testbed can facilitate this analysis for a reasonable cost.

## 4.2 Pedagogy

The testbed will play a significant role in teaching techniques in SCADA system classes such as PLC programming, forensics, etc., of these systems. In particular, it has substantial use in a graduate level course on SCADA/industrial control system security, recently introduced in the Department of Computer Science at the University of New Orleans.

**Demonstration of physical processes.** The testbed provides convenient access of three physical processes to students in a classroom setting, allowing them to observe and comprehend functionality of a physical process at a small scale. For instance, gas pipelines are generally spread over hundreds of miles, and so visiting the location of a pipeline is cumbersome and may not necessarily let students to observe the functioning of the system. The testbed covers critical functional aspects of the pipeline process and demonstrates to students how the controller in the pipeline maintains gas pressure.

**Varied programming software support.** The testbed uses the PLCs of three vendors, each using different programming software for their PLCs. It has SoMachine Basic, Studio 5000, and SIMATIC STEP 7 provided by Schneider Electric, Siemens, and Allen-Bradley. The students can thus learn and experience ladder logic programming on multiple programming softwares. SoMachine Basic also supports the Instruction List language for PLCs.

**Varied SCADA protocol support.** The testbed uses three popular SCADA protocols: EtherNet/IP, Modbus, and PROFINET. To gain a good understanding of a SCADA system and its associated physical process, students are often required to have good knowledge of relevant protocols. Students can capture network traffic of the testbed (such as on Wireshark [8] or NetDecoder [3]) and observe and learn the exchange of packets and their format.

# 5 Limitations

This section describes the limitations of the testbed including limited number of PLCs and the support of fieldbus I/O.

**No fieldbus I/O support.** The testbed does not support fieldbus I/O to connect actuators and sensors with a PLC. Currently, the sensors (such as the pressure gauge and the flow sensor) and actuators are connected directly with the input/output physical ports of PLCs. In industry, fieldbus is commonly used to simplify system expansion and modification; and also reduce the cost in wiring, connections, junction boxes, cabinets, and cable. Fieldbus protocols (such as ControlNet, and PROFIBUS) are used to exchange data between PLCs and actuators/sensors. They also provide remote access directly to actuators/sensors for diagnostic and debugging. Thus, fieldbus is critical for researching the lowest level of SCADA system i.e. actuators and sensors. It increases the attack vector for better evaluation of research prototypes. An adversary may directly target sensors and actuators and manipulate their data via number of cyber attacks including man-in the middle and denial of service attacks

**No connectivity with the cloud.** The current testbed consists of an isolated network that runs SCADA services on physical machines and has no connectivity with the cloud. Increasingly, SCADA systems are connected via cloud infrastructure, and the services are moved to virtual machines in a cloud infrastructure. The cloud offers several opportunities for developing novel solutions to secure SCADA services, and perform forensic investigation. For instance, SCADA services may be hardened at hypervisor level in a private cloud, and virtual machine introspection may be used for live forensics of SCADA services.

**No IoT appliances in the testbed.** The Internet of Things (IoT) is an emerging trend in the computing world, and is also encroaching upon industrial automation (coining a new term: industrial internet of things, or IIoT). The prevalence of IoT devices in industry brings unique cyber security and forensic challenges, such as whether IoT devices broaden the attack surface of SCADA systems; whether IoT devices and SCADA systems can coexist together without compromising their availability, integrity, and confidentiality; or whether existing digital forensic tools are sufficient to investigate IoT devices. Unfortunately, the current testbed lacks IoT devices for research.

# 6 Related Work

There are a number of ICS/SCADA testbeds in existence. The testbeds surveyed generally are full-scale functional sites; small-scale physical models; or primarily software-simulated models, occasionally with some physical equipment such as PLCs integrated into the simulation.

## 6.1 Small-Scale Physical Models

Mississippi State University built a similar small-scale physical testbed [21] with a water storage tank, a raised water tower, a factory conveyor belt, a gas pipeline, and an industrial blower on a serial control network, and a steel rolling operation and a smart grid transmission control system on an Ethernet network–these systems demonstrate the difference in need for security in serial vs. Ethernet networks. The serial network shares a single HMI system, and it implements remote

communication from the HMI through a UART MTU, connected to a 900MHz radio, which acts as a repeater for the serial network.

Iowa State University created the PowerCyber testbed [4], a simulated power grid that models two substations as two overcurrent relays each connected to a single Opal-RT RTDS (Real-Time Digital Simulator) as well as to two software-based RTUs that communicate through TCP/IP to a control center with a primary and backup HMI as well as a historian. Also included is a DigSILENT simulation attached to a number of RTUs also connected to the control center.

Researchers at Binghamton University [18] developed a power-generation testbed consisting of Allen-Bradley PLCs, AC and DC motor pairs to simulate electricity generation, and HMI. The system communicates using EtherNet/IP.

Researchers at Singapore University of Technology and Design [20] developed a small model water treatment system, titled "SWaT" (Secure Water Treatment), that is designed as a six stage model utilizing a primary and backup PLC on each stage. The PLCs utilize sensors to check water levels, chemical properties of water, and similar, while actuators are used to control pumps and valves. The system communicates with EtherNet/IP and Common Industrial Protocol, with EtherNet/IP tags used for sensor values and actuator settings, and the system is designed to allow for a choice between wired and wireless communication. The HMI system used is Allen-Bradley PanelView Plus. The physical process, HMI, SCADA system, and the historian are all interconnected with a switch.

Foo *et al.* [14] describe a testbed that they have developed at Queensland University of Technology and intend to use for practical security exercises. Similar to that at Mississippi State University, the testbed is a small-scale physical model of physical processes that includes physical PLCs, a VMware ESXI server, and networking equipment. The laboratory models “a water reservoir system, a pressurized pipeline, a conveyer belt system and a smart meter system.” The VMware server and network can be configured for a number of setups such as a corporate network as well as HMIs or PLC emulation.

## 6.2 Full-Scale Physical Systems

The National SCADA Test Bed is a multi-site resource supported by a number of labs supporting more than a dozen sites [1] with full-size equipment such as a power grid primarily at Idaho National Laboratory [2]. Pacific Northwest National Laboratory has a SCADA laboratory that can be used to test vendor products, system communication, and other systems [19]. This collaboration provides for tests on to-scale equipment for research by system owners, vendors, government, and other entities.

## 6.3 Software Simulations

Genge *et al.* [16] describe a software simulation using Emulab and Simulink to connect a software simulation of physical processes to a control network emulated in software representing PLCs and SCADA servers. The system uses both synchronous and asynchronous code to run the core simulation as well as simulated remote PLCs and processes.

Chabukswar *et al.* [10] utilize Command and Control WindTunnel [22] to combine a number of models simulating a plant implementing a simplified Tennessee Eastman challenge. The system includes a Simulink model and NetworkSim, each incorporated into the WindTunnel environment.

Davis *et al.* [12] created a simulated system using a PowerWorld server to simulate a power grid communicating with network clients. The network client is an HMI controller that communicates with the server with a simple protocol built upon TCP/IP. To model a larger network, the authors utilize RINSE, a network simulator and emulator, to act as a network simulator connecting network clients and the PowerWorld server. The client communicates to the PowerWorld server via a proxy server that relays traffic to RINSE through a VPN tunnel, which generates corresponding packets that will be sent by the proxy server to the PowerWorld server. By simulating nodes and connectivity with RINSE combined with PowerWorld, large scale power grid attack simulations can be studied.

### 6.4 Hybrid Models

Gao *et al.* designed the EPS-ICS testbed, a system that models a control process utilizing a "team boiler, water tank, and heat exchanger" [15]. The researchers designed a network testbed for corporate and SCADA network emulation, used physical PLCs, RTUs, and DCS controllers to interact with the process. Finally, MATLAB/Simulink was used to model the physical processes.

## 7 Conclusion

The testbed was recently built at the University of New Orleans using standard industrial equipment. Such an approach is generally more expensive than software simulations, and virtualized environments. However, it makes the testbed more closely representative of the real-world SCADA systems. The testbed has fully functional physical processes which is critical for research and pedagogical efforts.

## References Cited


[1] National SCADA test bed. http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/NSTB_Fact_Sheet_FINAL_09-16-09.pdf.

[2] National SCADA test bed. https://factsheets.inl.gov/FactSheets/idaho-test-range.pdf.

[3] NetDecoder. http://www.fte.com/products/NetDecoder.aspx.

[4] Power infrastructure cybersecurity laboratory. http://http://powercyber.ece.iastate.edu/powercyber.html.

[5] Profinet. http://us.profinet.com/technology/profinet/.

[6] EtherNet/IP. https://www.odva.org/Technology-Standards/EtherNet-IP/Overview, 2016.

[7] Modbus. http://www.modbus.org/, 2016.

[8] Wireshark. https://www.wireshark.org/, 2016.

[9] Irfan Ahmed, Sebastian Obermeier, Martin Naedele, and Golden G. Richard III. SCADA systems: Challenges for forensic investigators. *IEEE Computer*, 45(12):44–51, December 2012.

[10] Rohan Chabukswar, Bruno Sinópoli, Gabor Karsai, Annarita Giani, Himanshu Neema, and Andrew Davis. Simulation of network attacks on SCADA systems. In *First Workshop on Secure Control Systems*, 2010.

[11] Thomas M. Chen and Saeed Abu-Nimeh. Lessons from stuxnet. *IEEE Computer*, 44(4):91–93, April 2011.

[12] C. M. Davis, J. E. Tate, H. Okhravi, C. Grier, T. J. Overbye, and D. Nicol. SCADA cyber security testbed development. In *38th North American Power Symposium*, September 2006.

[13] Samuel East, Jonathan Butts, Mauricio Papa, and Sujeet Shenoi. A taxonomy of attacks on DNP3 protocol. *Critical Infrastructure Protection III, Springer*, pages 67–81, 2009.

[14] Ernest Foo, Mark Branagan, and Thomas Morris. A proposed Australian industrial control system security curriculum. In *46th Hawaii International Conference on System Sciences*, January 2013.

[15] Haihui Gao, Yong Peng, Zhonghua Dai, Ting Wang, and Kebin Jia. The design of ICS testbed based on emulation, physical, and simulation(eps-ics testbed). In *Ninth International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, October 2013.

[16] Bela Genge, Igor Nai Fovino, Christos Siaterlis, and Marcelo Masera. Analyzing cyber-physical attacks on networked industrial control systems. In *Critical Infrastructure Protection V: 5th IFIP WG 11.10 International Conference on Critical Infrastructure Protection, Hanover, NH, USA, March 23-25, 2011*, 2011.

[17] Peter Huitsing, Rodrigo Chandia, Mauricio Papa, and Sujeet Shenoi. Attack taxonomies for the modbus protocols. *International Journal of Critical Infrastructure Protection, Elsevier*, 1:37–44, December 2008.

[18] Emrah Korkmaz, Andrey Dolgikh, Matthew Davis, and Victor Skormin. Industrial control systems security testbed. In *11th Annual Symposium on Information Assurance*, 2016.

[19] Pacific Northwest National Laboratory. Cyber security: Protecting our nation's infrastructure. http://eioc.pnnl.gov/research/cybersecurity.stm.

[20] Aditya P. Mathur and Nils Ole Tippenhauer. SWaT: A water treatment testbed for research and training on ICS security. In *International Workshop on Cyber-physical Systems for Smart Water Networks*, 2016.

[21] Thomas Morris, Rayford Vaughn, and Yoginder S. Dandass. A testbed for SCADA control system cybersecurity research and pedagogy. In *Proceedings of the Seventh Annual Workshop on Cyber Security and Information Intelligence Research*, October 2011.

[22] Himanshu Neema and Janos Sztipanovits. Multi-model simulation: The command and control (c2) wind tunnel. https://www.nist.gov/sites/default/files/documents/el/building_environment/mechsys/Vanderbilt-C2WT-Sztipanovits.pdf, 2015.