Proc. of the 29th International Conference on Computer Application in Industry and Engineering, pp. 139 - 144, Denver, CO. September 26-28, 2016.

Cybersecurity Testbed Experimentation of a Resilient Control System for Power Substations

Charles Kim
Howard University
Washington, DC
ckim@howard.edu

Karen Green
DC Water and Sewer Authority
Washington, DC
Karen.green@dcwater.com

Andre Duarte Palhares
Pontificia Universidade
Catolica de Minas Gerais
potew0@gmail.com

Abstract

This paper focuses on the vulnerability of cyber-attacks to the open, connected control systems engaged in safety-critical applications and on the resilience of a newly proposed control system which is principled around diversity in hardware architecture. Our research has conducted vulnerability assessment of the existing control systems and validation of resilience of the new control system using two methods: lab hardware experiment and network simulation. This paper reports the result of the network simulation on a cybersecurity testbed, DeterLab. The paper briefs first on the architecture of the diversified computer control system and then details the cybersecurity testbed simulations for existing and new control systems presumably deployed for power substation applications. The DeterLab simulation demonstrates the cyber-resilient and fail-operate characteristics of the new diversified-hardware control system against cyber-attacks.

1 Introduction

The rapid spread control systems on open network architecture provide the benefit of operational convenience; however, unfortunately, it opens the door for malicious attacks, a success of which would mean a harmful access into the firmware and control functions, and consequently jeopardize the safe and normal operation of the application and threaten the public safety. Securing the network and communication to which these devices are interfaced are a great challenge for a safe and reliable operation of networked control systems.

One important application area of networked control system is nation's power grid which has evolved to a "smart grid", in which computer and communication technologies are being deployed rapidly to monitor and control generation, distribution, and consumption of electric power [1]. Examples of these monitoring and control devices include smart meters, phasor measurement units, and computer relays. Computer relays read from sensors of voltage and/or current and signal for controlling circuit breaker opening or closing. These intelligent electronic devices are networked, as remote terminal units of a supervisory control and data acquisition system, which in turn is connected to an enterprise network or energy management system. Managers and engineers of energy management system are allowed to operate networked devices and, when necessary, revise or update their settings or firmware. The advantages afforded by remote access has necessitated the use of Internet and wireless networks, and subsequently, data and control networks are no longer "air-gapped" but are connected to the network. This open connectivity has resulted in an increase in security vulnerabilities [2]. Unfortunately, the cybersecurity measures developed for detecting and preventing attacks do not work perfectly and are poor against new attacks vectors and viruses.

As a countermeasure for the networked control systems, a diversified control system was proposed so that a control system becomes fail-safe and cyber-robust even under compromised situations. Subsequently, the proposed new system was tested in simplified lab hardware setup with a staged remote access attack, and the experimentation has demonstrated its resilience and fail-operate characteristics [3]. This paper focuses on the further validation of the new control system architecture on a cybersecurity testbed.

The arrangement of the paper is made as follows. Section 2 discusses about the present control systems and their vulnerabilities. In Section 3, we brief on the new control system architecture which aims to be insensitive to the cyber activities. Section 4 details about a cybersecurity testbed DeterLab and our simulation of the new networked control system. Then Section 5 concludes the paper.

2 Existing Networked Control System

As computer and communication technologies have transformed once stand-alone devices to Internet-based networked control systems, major components in the smart-grid substation systems have become highly sophisticated with advanced operations and remote control functions. However, some of the newly developed communication networks have many flaws in security within its structure including weak encryption for user authentication [4, 5] and exposure to denial of service attacks. In addition, the two-way communication methods

978-1-943436-04-0 / copyright ISCA, CAINE 2016
September 26-28, 2016, Denver, Colorado, USA

adopted in the devices poses additional vulnerabilities of infiltration to the system.

A simplified representation of the existing control system in a power station is illustrated in Figure 1. The corporate-level energy management system (EMS) is connected to the substation via the Internet. The communication serve in the substation network connects the substation devices to the Internet. The EMS monitors multiple substations, and off-site managers and engineering staff can remotely login and access the substation system to control and monitor the substation devices such as digital relays.

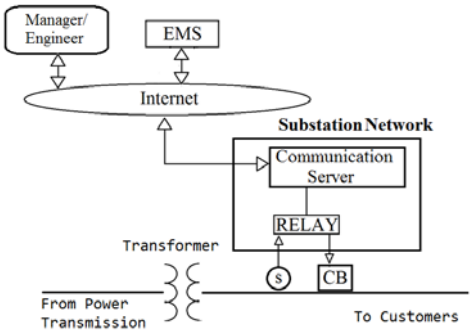

Figure 1. A simplified representation of the existing networked control system for power substation.

The digital relay (RELAY) in the figure is usually built on a computer which executes a program that is coded for specific functions. If the relay is programmed to be an overcurrent protective device, it reads the current level from the current sensor (S) and, by the programmed threshold setting, sends out an actuation command to the circuit breaker (CB) to open or close.

As for vulnerability, the access of the manager/engineer via Internet to the substation is the primary entry point for attack. After gaining the login credentials of the communication server, the attacker easily accesses the relay and may alter, for example, the threshold setting, which may cause an unintended operation for the substation. It would also have a direct impact on much wider power network as the unmet customer load of the compromised substation would have to be redistributed from other power stations. This possibility of ripple effect calls to mind Federal Energy Regulatory Commission's finding that the U. S. could suffer a coast-to-coast blackout if just nine out of the country's 55,000 transmission substations were knocked out on a summer day [6].

3 New Diversified Networked Control Systems

The new networked control system conceptualized and tested in a lab experiment setup was first conceived to make a control system cyber-robust and fail-operate against cyber-attacks which are assumed to compromise all the cybersecurity barriers implemented for the devices and networks [3]. The principle applied to the new system is centered on two principles: diversified redundancy in hardware and software; and unidirectional network connection from the control systems to the corporate-level network. A schematic of the diversified control system architecture is illustrated in Figure 2.

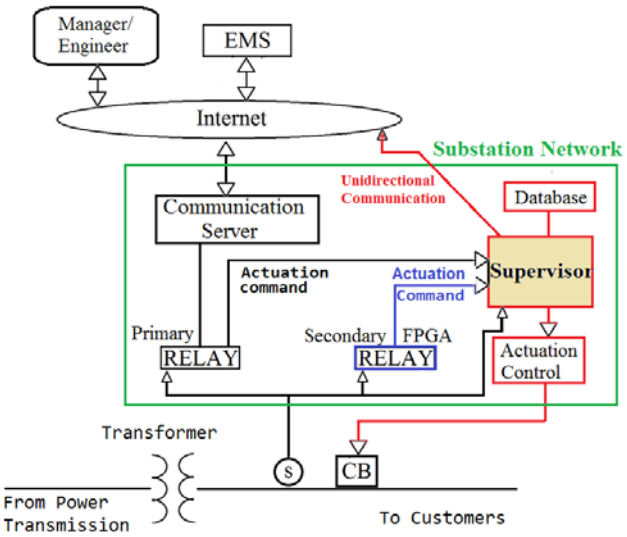

Figure 2. Diversified architecture for new networked control system for power substation.

The new system contains, in addition to the existing primary networked processor-based relay, a new secondary isolated relay which functions, in sensing the current level and generating signals for CB operation, the same as the primary relay but is built on different hardware such as field programmable gate array (FPGA) and on wired-code environment. In addition, there is a supervising controller ("Supervisor") which is built on either a processor-based or a hard-wire system. The Supervisor is also isolated from the network and is in charge of the eventual control of the CB. For CB actuation, the Supervisor monitors the CB control signals of both relays and decides if either one is wrong or not corresponding to an expected output based on the database server which collects normal operational current levels and corresponding CB operations.

If the Supervisor determines that the output from the primary relay is incorrect, it selects for correct CB operation that of the secondary relay, and at the same time, it sends a warning message to the EMS via a unidirectional communication network (via fiber-optic cable for instance) as this is indicative of a cyber-attack and infiltration to the primary relay. The unidirectional communication measure inherently blocks any possibility of receipt of any external command and of acting on such command [7]. More details about this new networked control system are found

in the reference [3]. The next section details the DeterLab testbed experiments for the existing and the new networked control systems and their analyses.

4. Validation in Cybersecurity Testbed

4.1 DeterLab

For the verification via software simulation, we decide to use a cybersecurity testbed known as DeterLab (cyber DEfense Technology Experimental Research Laboratory). DeterLab is a test facility for conducting critical cybersecurity experimentation and educational exercises. It emulates real world complexity and provides capability to research, experiment, and test cyber-attacks and defense technologies [8]. It provides over 400 computer nodes, with up to 10 network interfaces per node, each of which can support multiple apparatus elements by using virtualization techniques [9]. In a 2013 statistics, out of 209 active projects, six relate to power grid projects and two to control systems [10].

To create a DeterLab experiment, the NS (Network Simulator) format is used to describe the topology in setting nodes, defining links and the LAN which connect the nodes with specified bandwidth, latency, and que type, and specifying operating systems in the nodes. The NS also allows protocol options to route communication among the nodes. In order to run desired experiments, the nodes are to be accessed remotely from a local machine to view and manipulate or install software on the DeterLab nodes.

Connection to the nodes is done using Secure Shell (SSH) in conjunction with Windows Remote Desktop Connection client [11]. For remote connection, we use Putty, a free SSH client, for this experiment, to establish a forwarding tunnel to the remote GUI access port (3389, the port that Windows uses for remote GUI access) on the target Windows machine. A chosen port number on the local machine (6789) is corresponded to port 3389 on the remote machine using port forwarding.

Here is how to set up for tunneling and port forwarding (local 6789 to remote 3389) using Putty to connect to the nodes of the DeterLab experiment using remote desktop connection on Microsoft Windows. To configure Putty, the following is typed under the Host Name box of Session tab:

```
users.isi.deterlab.net
```

And on the "SSH>Tunnels" tab, `6789` is typed in the "Source port" field, the following project (for the experimentation) and port is typed in the "Destination" field:

```
EMS.proposed.scada-sc.isi.deterlab.net:3389
```

After the above step, the connection is established, and a terminal window is opened which indicates connection to the SSH target, DeterLab's "users" machine [12].

The final step is to connect to the remote GUI access port of Windows machines with a remote GUI access client, such as Remote Desktop. After opening the remote desktop from a local machine, an IP address and the port number is entered to the "Computer" field as follows:

```
Computer: 127.0.0.1:6789
User Name: None Specified
```

Then the Windows login dialog of the remote computer appears in the local machine, and login is accomplished using the Windows username and password of the machine. After this Deter nodes are accessed as if they are located in the local machine. The home directory is automatically mounted via Network File System (NFS) on every node in the experiment as well as the project directory during swap-in. Files are uploaded to the Deter host (`users.isi.deterlab.net`) using Secure copy (SCP) or SSH File Transfer Protocol (SFTP) [13]. WinSCP, a free SCP/SFTP client, is used for this experiment.

4.2 DeterLab Experiment with Existing Control System

To build an experiment for the existing networked control system, we start with modeling of the system and then create a user interface to show the response of the system under cyber-attacks. The network topology of the system modelled in DeterLab is illustrated in Figure 3. We represent the EMS, the communication network server, and the primary relay as the following three nodes, respectively, connected through LAN to Internet: EMS node, Router node, and Relay node. Since this is a virtual environment, all nodes are reserved with Class-A IP addresses. The Relay has a software code to work as an overcurrent relay with a threshold setting.

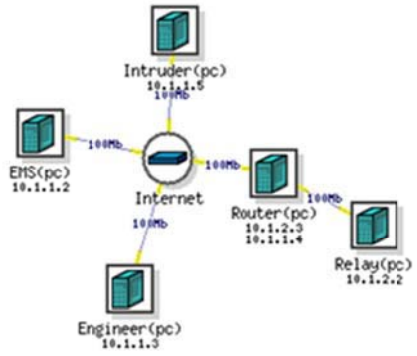

Figure 3. Existing control system topology on DeterLab.

Although the DeterLab's topology shows as if each of the three devices in the substation has an IP address, only the EMS is part of the TCP/IP network with the address 10.1.1.2. Two additional network devices in the topology are the Intruder node with an IP address of 10.1.1.5 and the Engineer with an address of 10.1.1.3 for the purpose of staging attacks. The operating system for each of the nodes in the network topology is set with Microsoft Windows.

The sensor (S) and the circuit breaker (CB) are not shown in the network topology because they are physically connected to the Relay without communicating directly to the Router. It is impossible in DeterLab environment to include non-network devices to the experiment; therefore, the reading from the sensor is entered manually in the experiment. This is the reason why we need a user interface. Similarly, the operation of the CB is shown through the user interface.

The user interface is developed using Visual Basic on the EMS, to which the Engineer has legitimate access to the Relay for threshold setting and others. The interface code examines the Relay setting and reads the sensor via manually entered values. It also displays the CB operational status determined by the Relay. Figure 4 illustrates a user interface screen which shows, at the top, the threshold value setting/display window and execution button of the setting to the Relay. Below are the window in the left for manually entering a sensor value, and the one in right for displaying the CB operation command.

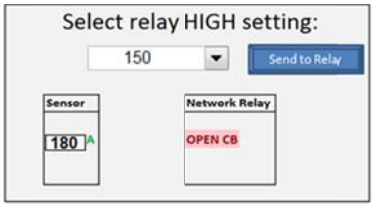

Figure 4. User interface for a sensor and Relay status.

Staging an attack to the network and corruptly changing the CB operational threshold of the Relay by the Intruder in the network simulates an ill-intentioned individual's unauthorized control over the system. The Intruder may use a Remote Administrative Tool (RAT) and infiltrate the system and change Relay configuration files on the Engineer for illicit modification of CB operational setting. RAT is classified as a virus called Trojan horse program, which typically carry payloads or other malicious actions that range from the mildly annoying to the irreparably destructive. They may modify system settings to start automatically [14].

A RAT is used in the following common structure: it has both a client (installed on the intruder's machine) and a server module (installed on the victim's machine). The server has a process that initializes as the system boots up and keeps running in the background, waiting for the client to connect. When the intruder wants to remotely manage or control the server, he launches the client on his machine. If the remote computer is powered up and connected to the Internet, then controlling is possible.

This DeterLab experiment considers a scenario in which a negligent engineer who has the authority to access the EMS computer executes a program that covertly installs the server module of the RAT on the Engineer computer. Further, an attacker connects to the Engineer computer where the server module is installed, the hacker can easily access the EMS and modify the setting and execute the altered setting to the Relay. The following screen display shows, after creating a tunnel using Putty and forwarding the desired ports as discussed above, the infiltration by the RAT in the DeterLab experimentation, in which an attacker in his local machine (IP 192.168.1.120) attempts to control the Engineer (IP 10.1.1.3):

```
>ipconfig
Ethernet adapter Local Area Connection 10:
Connection-specific DBS Suffix: isi.deterlab.net
IP Address: 192.168.1.120

Ethernet adapter Local Area Connection 6:
Connection-specific DBS Suffix:
IP Address: 10.1.1.3
```

Now the attacker accesses the EMS from the local machine and subsequently alters the setting for CB operation, for example, from 200 [A] to 150 [A].

Using the user interface illustrated in Figure 4, we explain how the CB operation is faltered by the hacker's modification of the setting. As shown in the Sensor window, the reading of the sensor is 180 [A] which is manually entered for testing; therefore, the correct operation of CB by the Relay is to be remained CLOSE. However, because of the altered setting for CB OPEN at 150 [A] from the attack as displayed in the top window, at the normal current level of 180 [A], the Relay sends out OPEN signal to the CB as indicated in the bottom right window.

The above example is a common type of cyber-attack which can disrupt existing control systems. A hacker can easily adapt this or similar approach to infiltrate any basic single-unit networked devices.

4.3 DeterLab Experiment with New System

The DeterLab experimentation for the new diversified control system is performed similarly. The new system is modelled in to a heterogeneous network topology with two additional devices: the secondary relay and the Supervisor. Also, to the existing communication network which connects the primary relay, a new network is added for Supervisor network which connects the Supervisor and the Database. Figure 5 illustrates the DeterLab network topology for the new control system.

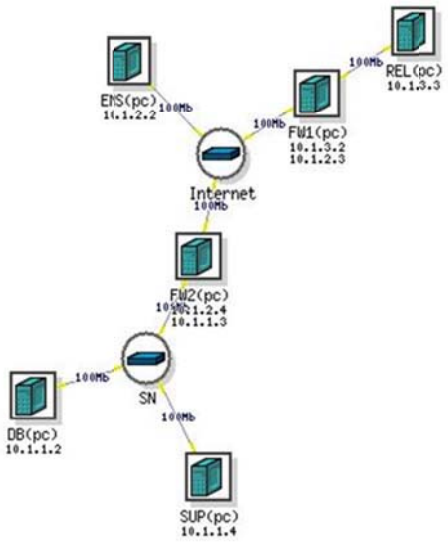

Figure 5: DeterLab topology for new control system.

As with the existing system, EMS is connected to the Internet, and the primary relay (REL) is connected to the Internet via a firewall (FW1). The supervisor network (SN) connects the Supervisor (SUP with IP Address 10.1.1.4) and database computer (DB) to the Internet via another firewall (FW2). As before all nodes are with Windows operating system. The sensor, the CB, and the secondary relay of FPGA are isolated from the network, so they are not represented in the topology. Their values and responses are simulated with a slightly revised user interface from the one used for the existing system experiment.

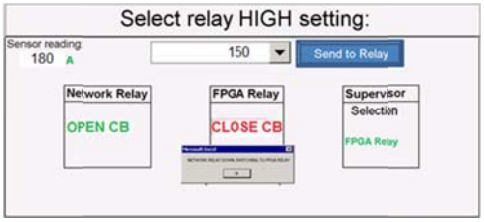

Figure 6. User Interface Developed for the Diversified Control System

The new user interface as illustrated in Figure 6, adds two relay response windows for CB operation and the Supervisor's window for CB control selection. The top window for setting alteration and the primary relay execution button are remained the same. The small pop-up window just below the secondary relay window will be explained shortly.

Now using Figure 6, we explain how the new control system survives under a cyber-attack. Let's assume that, by the same procedure of the RAT used for the existing system experiment, a hacker in his machine accesses the EMS computer and then modifies the relay setting of the primary relay from 200 [A] to 150 [A] and clicks the button for execution. Then, the normal loading condition of 180 [A] would make the primary relay erroneously produce "OPEN" command for the CB. On the other hand, the secondary Relay which keeps the correct threshold of 200 [A] would produce the correct "CLOSE" command. The Supervisor backed by the normal operation Database would select the secondary relay's CB command as the actuation signal CB operation. And the supervisor's action is displayed in the pop-up window in the user interface with the following message:

```
NETWORK RELAY DOWN. SWITCHING TO FPGA RELAY
```

Simultaneously, the supervisor sends alert to the EMS of the compromise in primary relay. For this communication requirement from the Supervisor to EMS, an additional feature is developed utilizing a socket program [18], by which a message is transferred as a file. The program is composed of two parts: a server (`fileserv.exe` in EMS) and a client (`fileclient.exe` in Supervisor). When the client connects to the server, it sends the file name and the file contents, and the server, after accepting the connection from the client through a specific port, receives the file name, creates a file with the given file name, receives the file contents, and writes the contents to the created file.

To execute the program at the server (EMS), on a DOS command prompt, the command "fileserv.exe <port number>" is to be entered as, for example, shown below for port number 8907:

```
C:\reports>fileserv.exe 8907
```

On the client side (Supervisor), the command "fileclient.exe" <IP address of destination computer> <port number> <file name> is to be entered as, for example, as shown below for IP address 10.1.2.2 of EMS, port number 8907, and the file name PrimaryRelayDown.txt. Then a message is displayed for the transfer:

```
C:\reports>fileclient.exe 10.1.2.2 8907
   PrimaryRelayDown.txt
File name is: PrimaryRelayDown.txt
PrimaryRelayDown.txt was sent
```

Then, on the server (EMS) side, the following message is displayed:

```
Message received
```

Now the last feature further applied for the DeterLab experiment is to make the message transfer unidirectional so that there is no chance of infiltrating the Supervisor from outside. For this purpose, we use Windows Firewall and block all the ports and applications except for port

8907, the port that is used to send the message to the EMS as illustrated above.

To allow only port 8907 on the tab of "Add a Port" in the Windows Firewall on the Supervisor, we type the name for the port and the port number as follows:

```
Name: SUP-Message
Port Number: 8907
```

Then in the "Exceptions" tab of the Windows Firewall, we select only the above typed name.

We can see the effect of the above Firewall configuration first in trying to connect to the Supervisor and second in pinging to the supervisor. In the first case, when a computer tries to connect to the Supervisor, the connection is denied with the following message:

```
Remote Desktop Disconnected
This computer can't connect to the remote computer
```

In the second case, when a computer pings to the Supervisor, its pinging is denied with the following message:

```
C:\Documents and Settings\karwil>ping sup
Pinging SUP-SN [10.1.1.4] with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 10.1.1.4:
Packets: Sent= 4, Received= 0, Lost= 4 <100% Loss>
```

However, using Windows Firewall blocking all other ports except for port 8907 for unidirectional warning message transfer provides just a partial solution, because there is no capability of controlling inbound traffic through that port. The communication from the EMS to Supervisor may still be possible if the hacker discovers that port 8907 is open.

5 Conclusions

For a validation of the new networked control system, we use DeterLab environment and its network topology modeling, and conduct experiments. In addition to the DeterLab resources, other tools such as socket program, user interface, and Windows Firewalls are applied to include both networks and isolated components and unidirectional message transmission. RAT is used for staging attacks in the experiments. The experiments demonstrate how the new control system, with its secondary, isolated relay of FPGA and the supervisor's monitoring, maintains the normal operation when the primary relay is compromised by the remote attack. Currently we are working to develop an interface which would connect sensors, actuators, and the secondary controller with DeterLab so that the entire system works online without any manual intervention in experiments.

References

[1] "What is the Smart Grid?," U.S. Department of Energy, Available: https://www.smartgrid.gov/the_smart_grid. [February 2014].

[2] K. Stouffer, J. Falco and K. Scarfone, Guide to Industrial Control Systems (ICS) Security, 2nd revisions, June 2015. Available :http://nvlpubs .nist.gov/nistpubs/ SpecialPublications/NIST.SP.800-82r1.pdf.

[3] C. Kim and R. Jaglal,, "Cyber-Robust Connected Control Systems: Experimentation Results," CAINE 2016 companion paper, 2016.

[4] R. Langner, *Robust Control System Networks*, NY, NY: Momentum Press, 2012.

[5] Tim Yardley, Robin Berthier, David Nicol, William H. Sanders, "Smart Grid Protocol Testing Through Cyber-Physical Testbeds," *Innovative Smart Grid Technologies Conference*, Washington, 2013.

[6] "U. S. Risks National Blackout From Small-Scale Attack," The Wall Street Journal, March 12, 2014.

[7] Andrew Ginter, "Waterfall Security Solutions – Prepared Remarks", FERC 2016 Supply Chain Integrity Technical Conference, Washington, DC. January 28, 2016.

[8]DETER Team, "The Deter Project," [Online]. Available: http://www.deter-project.org/.

[9]DeterLab, "Projects that have actively used isi.deterlab.net," USC Information Sciences and University of Utah, 2012. Available: https://www.isi.deterlab.net/projectlist.php.

[10]DeterLab, "Projects that have actively used isi.deterlab.net," USC Information Sciences and University of Utah, 2012. Available: https://www.isi.deterlab.net/projectlist.php.].

[11]University of Southern California, "Connecting to a DETER node running Windows," Available: http://www-scf.usc.edu/~csci530l/instructions/lab-deter-winconnect.htm.].

[12]B. Mitchell, "Sockets and sockets - introduction to sockets,",Available:http://compnetworking. about.com /od/itinformationtechnology/l/aa083100a.htm. .

[13]DeterLab, "DETERSSH-DETER," Powered by Trac. Available: https://trac.deterlab.net/wiki/DETERSSH.

[14]"Trojan-Threat Encyclopedia," Trend Micro, USA, November 20, 2014