Cyber-Defensive Architecture for Networked Industrial Control Systems

Charles Kim
Electrical Engineering and Computer Science
Howard University
Washington DC, USA

***Abstract*—This paper deals with the inevitable consequence of the convenience and efficiency we benefit from the open, networked control system operation of safety-critical applications: vulnerability to such system from cyber-attacks. Even with numerous metrics and methods for intrusion detection and mitigation strategy, a complete detection and deterrence of internal code flaws and outside cyber-attacks has not been found and would not be found anytime soon. Considering the ever incompleteness of detection and prevention and the impact and consequence of mal-functions of the safety-critical operations caused by cyber incidents, this paper proposes a new computer control system architecture which assures resiliency even under compromised situations. The proposed architecture is centered on diversification of hardware systems and unidirectional communication from the proposed system in alerting suspicious activities to upper layers. This paper details the architectural structure of the proposed cyber defensive computer control system architecture for power substation applications and its validation in lab experimentation and on a cybersecurity testbed.**

Keywords- Component; Supervisory Control and Data Acquisition System, Smart Grid, Power Substation, Cybersecurity, Diversification, Testbed.

I. Introduction

Cyber incidences are ever increasing as they are expanded from simple bragging intrusion to monetary gains and exploitation to trading secret stealth and to military and national security espionage. One important area in the cyber incidences in which public are not keenly aware of is networked embedded computer systems for intelligent and autonomous control and processing applications including, but not limited to, smart power grid, water treatment and distribution systems, petro-chemical plants and refineries, and mobile and home automation systems, termed combined as Internet of Things (IoT).

The widely adopted IoT on open network architecture provides the benefit of economy of operation; however, unfortunately, it opens the door for unintended threats including malicious code manipulation, data gathering, and unauthorized intrusions into the network. A successful intrusion would allow attacks on operator consoles, and harmful access into control functions which would consequently disrupt normal operations and thus pose a public safety threat.

Presently, the hardening of system is heavily focused on the cyber security for information systems connected to the Internet, and there are numerous strategies and tools available, and are under development. Anomaly and intrusion detection, network access behavior analysis, modeling approach, mitigation are just a few of them. Understanding attack vectors is essential to building effective security mitigation strategies. Attack vectors include viruses, e-mail attachments, Web pages, pop-up windows, instant messages, and deception.

There are several common countermeasures proposed against attack vectors [1]. They include: (i) development and review of security policies; (ii) employment of blocking access to resources and services on the network; (iii) enactment and monitoring of detection of intrusion and malicious activities, (iv) implementation of mitigation against possible attacks, and (v) application of continuous fixing, upgrade, and patch the software vulnerability.

However, the countermeasures developed from metrics can block some attack vectors but are not totally attack-proof. They are backward-looking metrics and measures, analyzing only after an incident with subsequent damage has already occurred. Therefore, the metrics and measures and mitigations developed for the Internet and computer networks may not be effective in dealing with unknown malwares and vulnerabilities specifically targeted for safety- and mission-critical control system applications. The Stuxnet malware attack to an Iranian nuclear facility demonstrates that the reality of the vulnerability of safety-critical systems to cyber-attack is real, and that there will be dire consequences to critical infrastructure if such cyber threats are not detected and mitigated properly and timely [2].

Considering the impact and consequence of mal-functions in the safety-critical applications caused by cyber incidents, this paper proposes an architectural change in the way components are structured so that a networked control system becomes cyber-defensive and resilient even under compromised situations. The proposed system aims to be insensitive to variations in inputs, processes, and outputs of cyber contents. The proposed defensive architecture is centered on diversification of hardware systems and unidirectional communication to the energy management system for alerting suspicious activities. The rationale of the architectural approach against cyber threats is the plain truth that it is impossible to predict cyber events throughout the computer control system’s lifecycle, and that detection and mitigations strategies may be good for old and known malwares and viruses only [3]. Therefore, the methodology used in the proposed cyber-defensive architecture for power substation control systems focuses, assuming that an attack will occur, on designing a system that is robust enough in its response so that the effect of an attack will be minimal and the power substation can continue in serving customers and in protecting power systems [4].

The paper is organized as follows. In the next section, we discuss about the present computer control systems deployed in a power substation and their vulnerabilities. Then, we detail the proposed architectural approach with hardware and software diversity to be insensitive to the cyber inputs and activities, which would results in cyber-robust and cyber-resilient systems. After that, validation of the new architecture is examined on a cybersecurity testbed and in lab experimentation. Then, we conclude the paper.

II. Vulnerability of Industrial Control Systems

Over the past several years, power substation systems have become highly sophisticated in structure and operation, featuring various types of intelligent devices that allow advanced operation and control functions. Computer and communication technologies have transformed stand-alone computerized control systems to Internet-connected smart grid control systems. The smart-grid network provides a great benefit of situation awareness, data collection and analysis for operational efficiency, and coordination of automation and restoration of power networks [5].

A lot of the devices that constitute these smart systems are seen commonly more demanding sectors. Common examples of these devices include smart meters, phasor measurement units, and sensors (voltage and current monitors) and actuators (circuit breaker openers/closers). These “intelligent electronic devices (IEDs)” are networked, as remote terminal units (RTUs) of a supervisory control and data acquisition (SCADA) system, which in turn is connected to an enterprise network or energy management system from which engineers are allowed to operate IEDs and, when necessary, control request or resolve their problems. The advantages afforded by remote access has necessitated the use of Internet and wireless networks, and subsequently, SCADA networks are no longer “air-gapped” but are usually connected to their corporate network and internet through a firewall. This relatively open connectivity has in turn resulted in an increase in security vulnerabilities [6].

To illustrate a sample of the vulnerabilities of the current control and protection system in power substation, a representative diagram is given as Fig. 1. The diagram highlights a simplified representation of a power substation with a communication network (CN) server and a computer/digital relay is disposed for a circuit breaker operation. The enterprise-level energy management system (EMS) is connected to the substation via the Internet. The CN device connects the substation systems to the Internet where all of the engineering staff can login and access the system. The EMS monitors multiple substations via the Internet, and the flexibility of the network allows engineers to control and monitor the relay system from off site.

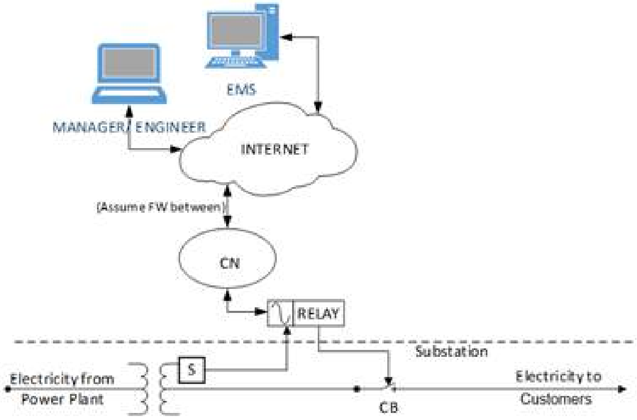


Figure 1. Simplified Representation of Present Power Substation System.

A current sensor (S) is attached to the relay, and based on the sensor reading, the relay can open the circuit breaker (CB) by sending a command signal to the CB actuator when it is necessary or in an emergency. The relay is built on a computer with a standard operating system such as Windows that executes a program that is coded for specific functions and features. When the relay is programmed as an overcurrent protective device, if the sensed current level is higher than a threshold, it would generate an “Open” signal for the CB actuator. It is assumed for our discussion that the relay is an overcurrent computer relay. In addition, a standard desktop computer labeled as ‘Manager’ with a designated operating system is connected to the relay via the Internet. This allows the individual responsible for overseeing the proper functioning of the system to manage and control the relay, should the need arises.

Now consider cyber vulnerabilities of the substation depicted in Fig. 1. First, the Internet connection represents a possible entry point for hackers to infiltrate the system. If a hacker can gather the appropriate login credentials of the communication network server, he/she can possibly gain access to the relay and alter its operating state. Once that party is logged into this system, they have free reign to enact whatever change they please, which we are assuming is to damage the system in some way. Any alteration to the relay may have major repercussions for the substation and the consumers served by the substation. It would also have a direct effect on surrounding substations as the load of the compromised substation would have to be redistributed amongst its neighbors. This possibility recalls the Federal

Energy Regulatory Commission’s finding that the U. S. could suffer a coast-to-coast blackout if just 9 out of the country’s 55,000 transmission substations are knocked out on a scorching summer day [7].

III. Cyber-Defensive Architecture

As mentioned above, there exist vulnerabilities in the present power substation and its network, and the countermeasures developed from the presently employed metrics are not attack-proof. Moreover, metrics and measures and mitigations developed for the Internet and computer networks may not be effective in dealing with unknown malwares specifically targeted for safety- and mission-critical control system applications. Even dynamic and learnable measures and metrics cannot possibly detect all and, particularly, unknown and new malwares and their tactics. Therefore there is a demand to make computer control systems robust against cyber threats and resilient under such cyber-attacks.

The proposed architectural approach aims to be cyber-insensitive, and the logic of the proposed defensive architecture is grounded in the concept of software and hardware redundancy/diversity and of utilization of unidirectional network connection. More specifically, the architecture is the result of combining the standard principles of diversified redundant hardware and software for defense-in-depth into a very efficient supplementary system that can integrate with the general structure of the systems currently in use.

A. *Diversified Redundancy and Defensive Architecture*

The use of redundancy design techniques is already an accepted practice when trying to address fault and failure scenarios in software and hardware. For example, most data is typically backed up to secondary storage spaces and synced as often as possible to ensure minimal to no operational disturbance in most industries. Also, critical manufacturing or generation processes are built with redundant hardware measures to allow easy replacement, repair and maintenance.

Redundancy is effective, but if a machine fails due to a virus attack, for example, then even the redundant machines will be susceptible to the same virus, if they are of the same hardware and software version. This common-cause failure would most likely damage both machines. If, however, the redundant machine has different hardware specifications, there is much greater probability that the redundant machine would survive against the same problem which has caused the primary machine to transition into a fail state. This difference in hardware (and software) is called diversity. Design diversity has also been a tried and true method employed to add a layer of protection to critical systems by protecting redundancy systems from such common-mode failures. Its range of application is vast and its representation can be in the form of software variants to actual physical design differences between primary systems and their redundancy counterparts.

A representative model of the proposed system architecture is illustrated in Fig. 2. In the proposed design, alongside the existing primary computer/digital relay (“RELAY”), there is secondary digital relay that functions, in sensing the current level and generating a signal for CB operation, identical to the existing one but built on different hardware such as field programmable gate array (FPGA) and run on a completely different software environment (“FPGA”). Unlike in the existing system, the CB operation signals from the two relays are monitored and selected by a supervising computer system (“SUPERVISOR”) which is built on a PC or a hard-wire system; therefore, the SUPERVISOR is in charge of the eventual control of the CB. As in the existing substation, the primary RELAY is connected to the communications network (CN), while the secondary FPGA is remained not connected to any network.

The SUPERVISOR is separated from the Communication Network, and reads the CB control signal outputs of both relays and decides if either one is erroneous or not by conferring with a database server which contains data readings collected at the sensors and the corresponding CB operations over an extended period of operational hours. Under regular operating conditions, there should be near perfect correlation for given sensed value between the CB control signal generated by the two relays and the cached CB operational mode in the database server.

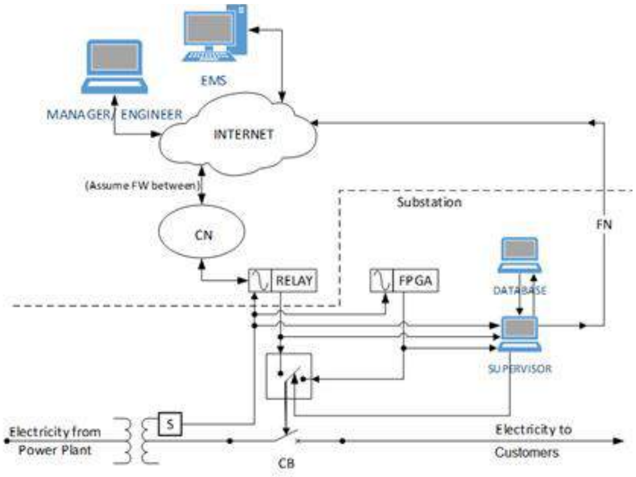


Figure 2. Defensive Architecture for Power Substation System.

In the event that the SUPERVISOR finds an inconsistency between the CB signal of the primary RELAY and the database, for example, it gives the CB operational control to the secondary FPGA relay which produces the correct signal. At the same time, it sends a warning message to the EMS via a unidirectional fiber network (FN) as this is indicative of the primary RELAY being possibly compromised, to alert the management personnel of the state of the system. The importance and distinct advantage of using unidirectional network connection is the fact that this new system at no point is required to receive and act on requests [10]. Hence, the integrity of alerting is preserved and the possibility of communication related intrusions such as Denial of Service (DoS) attacks is inherently prohibited.

B. *Qualitative Assessment*

Before we validate the new approach, let's do qualitative assessment of the new architecture on its claimed strength against cyber-attacks under a few instances, all feasible within the environment of power substation operations. First, we consider the presence of a common computer virus which gains entry into the system via a negligent substation engineer. Under these circumstances, the operation of the primary RELAY becomes compromised. The secondary FPGA relay on the other hand, by way of design diversity remains unaffected. Even in the instance of viruses that have the ability propagate across networks, the difference in programming methodology between the two relays grants mutual exclusion in the case of software attacks, eliminating the threat of common-cause virus infections.

The next attack scenario considered is a theoretically attempted man-in-the-middle attack. This scenario involves attacks in which access credentials are mined from unsuspecting parties. In this case, it is difficult to determine if the system is under attack because the information used to gain unauthorized access to the system is indeed legitimate. Therefore, changes can be made to the primary RELAY without any intrusion indicators being set off. But even in this highly compromised state, by virtue of the comparison check that occurs continuously at the SUPERVISOR, any changes or discrepancies generated by the intruder are flagged, and controlling of the substation functions is committed to the secondary FPGA relay.

Another considered scenario is an event of common hardware and software failures. Hardware failures in this context refer to incidents such as purposeful or accidental physical damage and hardware component faults, which cause eventual failure. The proposed architecture ensures that in case of damage to the primary RELAY, the secondary FPGA relay can function autonomously not being susceptible to common-mode hardware failure. This ensures that the service is maintained until the proper repair and replacement procedures can be carried out. While the probability of simultaneous failure of both the primary and secondary relays of the proposed system exists, it is theoretical and very small.

The last scenario we consider for qualitative assessment is with a mode of attack employed by a Stuxnet-like worm in its various iterations. The Stuxnet worm is a program that was developed to target specific industrial software on a specific brand of equipment in a plant [2]. This type of specialized attack is hard to defend from because it relies on targeting and exploiting certain vulnerabilities in the operating system. Fortunately, the design diversity afforded by the new system structure acts as a functional safeguard. Having both relays run on very different software and hardware architectures ensures that whatever damage is done is limited to the primary RELAY. The new solution architecture upgrades the existing system to a multi-tiered, cooperative system in which desired relaying functions are kept intact all the time fulfilling the response robustness required of systems that handle such critical task as power substation control and management.

To verify the feasibility and viability of the proposed architectural solution, two approaches are employed: simulation on a cybersecurity testbed and experimentation with hardware components. In both validation approaches, the representative models of the existing power substation system and the new defensive-architecture system are implemented in a network simulator and in a system of microcontrollers and FPGA, respectively. Then, the two models are subjected to the same attack conditions and the each response is recorded and analyzed. The testbed simulation is discussed in the next section, and the hardware lab experimentation follows in the section after the next.

IV. Validation in Testbed Experimentation

To accomplish verification via software simulation, a testbed known as DeterLab (cyber DEfense Technology Experimental Research Laboratory) is utilized. DeterLab is a facility for scientists engaged in new cybersecurity technologies. The Deter Team works with subject matter experts in specific areas of cybersecurity or critical infrastructure protection, and the DeterLab is a part of the work which provides real world capability to research, develop, discover, experiment on and test cyber defense technologies [9]. Approved users can access DeterLab's advanced resources and tools, and perform repeated, verifiable experiments. DeterLab 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 that support the experimenters' goals [10].

A. *Existing Control System Experimentation*

To demonstrate the vulnerabilities in the existing system of Fig. 1, we model the network topology as Fig. 3. The DeterLab evaluation begins with conceptualizing the model of the simplified primary Relay. The model is then created in DeterLab after which a user interface is created in DeterLab. A remote administrative tool (RAT) is used to show how an intruder can infiltrate the system and change Relay configuration files on the EMS. The RAT is classified as a virus called Trojan horse program, a malware which by itself is not capable of automatically spreading to other systems. Trojans are usually downloaded from the Internet and installed by unsuspecting users. They 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 [11]. As shown in Fig. 3, the model consists of an EMS, Intruder and Engineer nodes connected to the internet. The primary, networked Relay is connected to the internet through a Router (or firewall not shown).

In the topology of Fig. 3, since this is a virtual environment, all nodes are reserved with Class-A IP addresses. Although, in the DeterLab representation, each device in the substation has an IP address, only the EMS is part of the TCP/IP network, with the address 10.1.1.2. The Sensor and the Circuit breaker, not shown, are physically connected to the Relay without communicating directly to the Router.

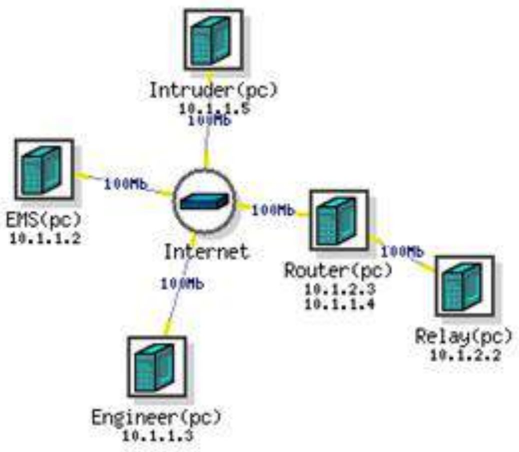


Figure 3. DeterLab Reprentation of the Existing Control System.

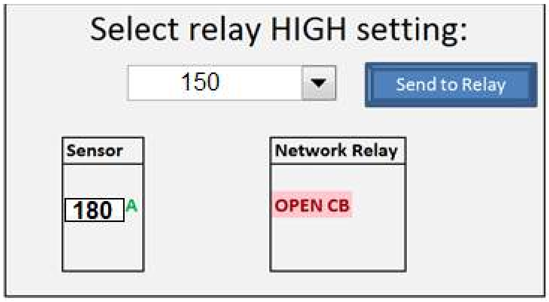
Other notable hosts include the Intruder node with an IP address of 10.1.1.5 and the Engineer with and address of 10.1.1.3. The Intruder and Engineer nodes are added to represent a hacker and an engineer in order to stage an attack, respectively. The Intruder in particular is added to simulate an ill-intentioned individual who wants to gain unauthorized control over the system. In order to do this, the Intruder may use a RAT. There are various types of RATs available, and most of them are made to be used with the consent from the owner of the controlled computer, but for our purpose, we will assume no permission is granted. Although various RATs are used for a range of purposes, their structure remains the same: 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 just launches the client on his machine. If the remote computer is powered up and connected to the Internet, then controlling is possible.

This DeterLab simulation considers the situation where a negligent engineer or manager, who has the authority to access the EMS computer remotely, executes a program that covertly installs the server module of the RAT on his computer. Although most antiviruses easily flag these kinds of files, there are some techniques to make them fully undetectable. However, we will not cover them in this article. Instead, let us suppose the user has no updated anti-virus software installed on his machine and/or the hacker has encrypted his server on purpose.

By using PuTTY to create a tunnel and forwarding the desired ports (local 6789 to remote 3389), it is possible to connect to the nodes at DeterLab using remote desktop connection on Windows. In order to gain this control, the hacker must force the user to execute a file that will automatically install the server module. He can do it by using techniques known as social engineering, that is, by persuading the user to download and execute the file.

Considering that the RAT is a Trojan which can be disguised as a legitimate software component, if the Trojan's configuration complies with the substation network, it will silently enable the remote control, without the victim's (engineer or manager) consent or acknowledgment. On whichever machine the file is run, either the EMS or the Manager/Engineer's computer, it will install the server module. Once connected, the hacker can easily modify any file in the remote system. The RAT used in this network gives the user the possibility to download, modify and upload a file on the host computer. In other words, in power substation, software for controlling the Relay and for activating CB can be modified without the operator's noticing.

To demonstrate how the modification of the threshold value for CB opening by attacks changes the CB signal from the Relay, a user interface is developed using Visual Basic on the EMS. For the interface, since the current sensor cannot be included in the network topology, the reading from the sensor is entered manually, and the CB operational threshold ("HIGH" as illustrated of the interface in Fig. 4) is stored in a file on the primary Relay. Under a compromised situation via RAT attack, the setting for HIGH may be changed from 200 to 150, for example. Then, even under the normal current level of 180 at which the circuit breaker normally remains closed allowing power supply to the customer, the Relay sends out OPEN signal to the CB by the altered threshold of HIGH to150 from 200.


Select relay HIGH setting:

150

Sensor

180 A

Network Relay

OPEN CB

Figure 4. Response of the Network Relay by the RAT attack.

The illustration made above is a common type of cyber-attack and currently infects thousands of computers around the world. A hacker can easily adapt this tool to infect IEDs from someone who possesses high privileges in an electric power company. The executable file can be encrypted or bended to other file or spread through other known means in order to reach its final target. Therefore, it is important not to depend on a single machine to control critical devices like digital protective relays, neither is it recommended to trust people with low awareness on the critical importance of cyber-security to operate this kind of equipment.

B. Defesnive-Architecture Experimentation

The DeterLab simulation for the proposed architecture is performed similarly. First, a model is conceptualized for the new architecture which includes a non-networked diversified redundant FPGA relay and SUPERVISOR. Second, a slightly different user interface is developed to display the response of the new system for primary Relay and secondary FPGA under the same RAT attack and relay threshold setting file modification. Third, it is shown how a message is sent from the SUPERVISOR to the EMS and how unidirectional flow of data is achieved between them.

Fig. 5 illustrates the topology model of the proposed diversified architecture in the DeterLab. The network topology is created using six nodes. The EMS is connected to the Internet. The primary Relay (REL) is connected to the Internet via a router or firewall (FW1). The other network in the model is the supervisor network (SN) which comprises of the SUPERVISOR (SUP) and database computer (DB). The sensor and the secondary FPGA relay are non-networked devices and thus are not represented in the topology, and their values and responses are simulated by manual entry into the user interface.

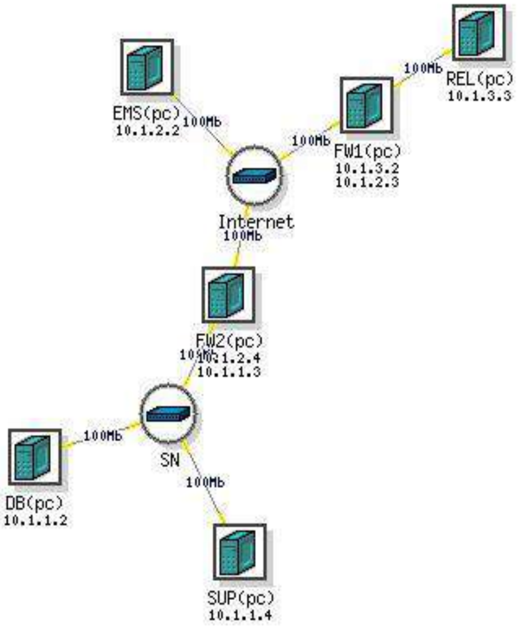
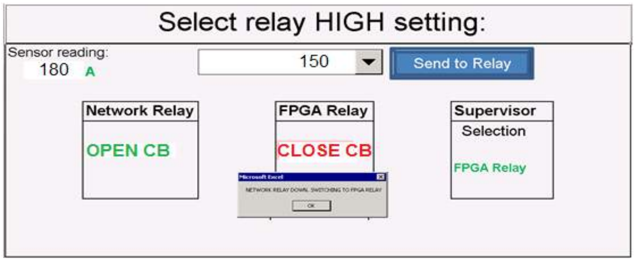


Figure 5. DeterLab Representation of the Defensive Architecture.

The same user interface developed for the existing system simulation is used with a slight revision to accommodate the secondary relay FPGA as illustrated in Fig. 6.


Select relay HIGH setting:

Sensor reading:
180 A

150

Network Relay: OPEN CB

FPGA Relay: CLOSE CB

Supervisor Selection: FPGA Relay

Microsoft Excel

NETWORK RELAY DOWN, SWITCHING TO FPGA RELAY

Figure 6. User Interface Display under an attack with modifed setting.

The FPGA Relay provides the same functionality as the primary network relay but with strong immunity against setting modification due to its hard-code environment. If the relay setting is changed by the RAT attack with altered threshold value as done before, from 200 to 150, for example, for the normal loading condition of 180 A, the network relay's output ("OPEN") does not match with the true output ("CLOSE"), and the selection of relays to control the circuit breaker will be switched to the FPGA relay with a message of such control transfer. Fig. 6 shows the switch to FPGA with a message in the user interface.

To demonstrate message delivery from SUPERVISOR to EMS of the abnormal and suspicious behavior of the primary network Relay, a socket program in C programming language is used [12]. The program is written in two parts: a server (fileserv.exe) and a client (fileclient.exe). The server accepts a connection from client through a specific port, receives the file name, creates file with the given file name, receives the file contents, and writes the contents to file. On the other hand, the client connects to the server, sends the file name, and sends the file contents. For the DeterLab simulation, the server module is executed on the EMS while the client module is executed on the SUPERVISOR.

Before executing the program, however, the fileserv.exe file is saved in a folder where the file is to be executed and the message is to be created and saved. Similarly, the fileclient.exe file is saved in a folder where the file is to be executed and the message is to be copied. In both cases, a directory called c:\reports is created. To execute the program at the server a DOS command prompt window is opened and the directory is changed to the c:\reports folder. On the server, the command "fileserv.exe <port number>" is entered. In this case port number 8907 is used. On the client, the command "fileclient.exe" <IP address of destination computer> <port number> <file name> is entered. In this case, the IP address is 10.1.2.2, 8907 is the port number, and NetworkRelayDown.txt is the file name.

Now the last subject of discussion is the unidirectional information transfer from the SUPERVISOR to EMS on reporting the abnormal and suspicious functioning of the primary Network Relay. For our simulation, the unidirectional flow from the SUPERVISOR is set up by using Windows Firewall to block all the ports except for port 8907, the port that is used to send the message to the EMS. All other ports and applications are blocked. The effect of the Firewall configuration is verified in that a computer is unable to connect to SUPERVISOR and unable to ping SUPERVISOR.

C. Discussion on DeterLab Experimentation

Modeling of the existing and the proposed substation systems are realized in DeterLab environment as network topologies with corresponding nodes with the Internet and routers and firewalls. It is shown that with an RAT, it is possible to gain control of a remote computer and change files on a remote computer, and the existing system sends out an erroneous command to the circuit breaker. On the other hand, the proposed architecture system demonstrates how the secondary FPGA is immune to the attack and the system itself keeps the normal operation mode by the SUPERVISOR's monitoring while the primary network relay, impacted by the changed setting, produces a wrong command to the circuit breaker. In addition, the message is successfully sent from the SUPERVISOR to the EMS using a socket program through TCP. This is achieved by manually triggering the program and setting the port number through which the message is sent. Unidirectional flow from the SUPERVISOR to the EMS is partially achieved using Windows Firewall blocking all other ports except for port 8907. However, the software is limited in that there is no capability of controlling inbound traffic through that port, which means that communication from the EMS to SUPEERVISOR may still be possible if the hacker discovers that port 8907 is open. Also, DeterLab seems to have a limitation in that when the SUPERVISOR is blocked using Windows Firewall, it is not possible to connect to it to do further testing. The experiment would have to be reset by swapping it out and then swapping it in again.

V. Validation in Lab Experimentation

This section discusses a small-scale hardware experimentation of the existing and the proposed new system. The aim here though is not to produce a physically scaled down replica, but to perform an extended version of tangible, logical validation and illustration. It should therefore be noted that the components used to achieve this hardware experimentation are neither directly relatable to the industry specific equipment in use, nor are they scalable. Specific details such as response times are not considered because they would largely be dependent on the precise equipment that would be used if this solution approach is adopted.

A. Lab Experimentation Setup

As for hardware components for the simplified substation systems, as illustrated in the schematic of Fig. 7, the primary relay is represented by an Arduino microcontroller [13] ("Primary Arduino"), the secondary FPGA relay by a Nexys II Spartan-3E FPGA board ("Secondary FPGA"), and the supervisor by an Arduino microcontroller with an attached Ethernet Shield ("Supervisor Arduino").

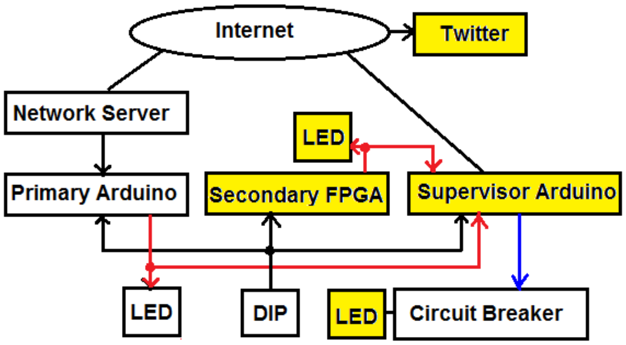


Figure 7. The Hardware Experimentation Components.

The communication server is represented with a laptop with Microsoft Windows 7 Professional operating system which is connected to the Internet. The Supervisor Arduino is also connected to the Internet, and a Twitter account, ArduinoHU, is made to represent the EMS and to simulate the message transmission upon a cyber-incident.

The current sensor is represented by a DIP switch by the position of each toggle of which can simulate various loading conditions. The circuit breaker is implemented by a simple magnetic switch/relay, the operation (Open/Close) of which is controlled by a digital command. An LED is attached to the magnetic relay to indicate the operation state of Open (ON) or Close (OFF). In addition to the LED attached to a circuit breaker representative, an LED is connected to each of the relay representatives to indicate the output status of it. The DIP is directly connected to an input port of both Primary Arduino and Secondary FPGA as well as to the Supervisor Arduino’s input port. The digital command to operate the magnetic switch is issued by the Supervisor Arduino from the outputs of Primary Arduino and Secondary FPGA, which are directly connected to the input ports of the Supervisor Arduino.

As for software, a simple code is programmed for the relay representatives for reading values from the DIP switch and sending out corresponding outputs based on the pre-set threshold value. The Supervisor Arduino is coded to take in two outputs and compare them to a database of past sensor readings and respective CB operations which is nothing but a simple table embedded in the code. Fig. 8 depicts the lab hardware experimentation set on a breadboard.

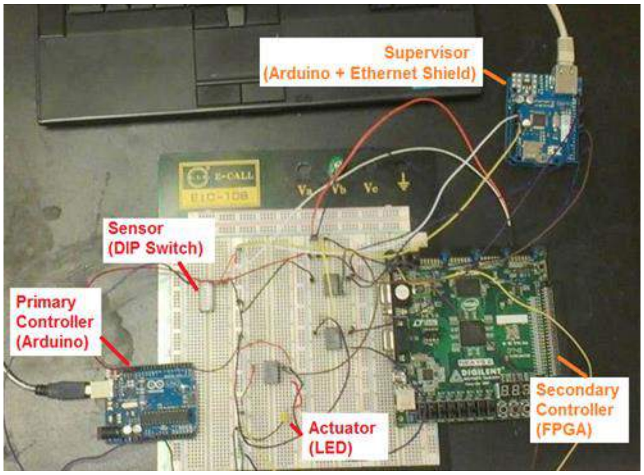


Figure 8. The Lab Hardware Experimentation Setup.

The simulation of the existing system is done on the experiment setup just by using only the network server and the Primary Arduino and the DIP switch (all unshaded components of Fig. 7), and that for the proposed system is done using all the components. In both cases, it is assumed that the attack is made through virtual private network (VPN) of the substation and that the attacker has access to the engineer's laptop after obtaining the credentials from the Trojan virus or using a key logger.

B. *Cyber Attack on Existing System*

Once the hacker has the credentials to the engineer's laptop which is connected to the substation network, the hacker easily connects, using the remote desktop tool in Microsoft Windows, to the remote communication network server which is also running a Microsoft Windows operating system. In the process, the hacker inputs the IP address of the remote machine and then he types in the credentials for the communication server, to which all IEDs within the substation including the relay (represented as the Primary Arduino in the setup) are connected. At this point the hacker has now access the application that programs the Primary Arduino, and can upload corrupted code to the Primary Arduino.

In this particular simulation, the hacker uploads a code which frequently changes the threshold value for circuit breaker operation from very low to very high, and it results in producing the constantly tripping and closing signals to the circuit breaker, manifested in the blinking LED every one second while the DIP switch positions are remained intact. Under this type of operation, the existing substation system components cannot survive and the service would be disrupted to the customers until the crew come to the substation and repair the problem and restore the service.

C. *Cyber Attack on the Defensive Architecture*

Now the same attack is staged for the system of the proposed architecture. Again, the amount of loading is simulated with the positions of the DIP switch and a certain threshold value is coded in to Primary Arduino and Secondary FPGA. Also, we assume that the hacker has already entered the network and placed the same corrupted code in Primary Arduino. Since the Secondary FPGA is not connected to the network and keeps its operational logic in its hare-wired code, it does not suffer from the attack. Therefore, while the Primary Arduino produces and sends erratic ever-changing outputs to the Supervisor Arduino, manifesting with flashing LED of its own, the Secondary FPGA sends consistent output based on the loading level. Now the Supervisor Arduino compares the two outputs against the normal operation history from its database, and selects the Secondary FPGA to control the circuit breaker, manifesting the state of the circuit breaker LED the same as that of LED of the Secondary FPGA.

Hence, even under the compromised situation in the Primary Arduino, the intended functions at the substation would survive and there would be no disruption of service to customers. At the same time the Supervisor Arduino sends a twitter message to a Twitter account, ArduinoHU, stating that the Primary Arduino has malfunctioned and alerting the engineers of the EMS to come on site to repair the compromised component. The proposed architecture has shown that it can survive cyber-attacks.

D. *Discussions on the Lab Hardware Experimentation*

The lab hardware experimentations with the remote attack scenario demonstrate the vulnerability of the existing system and a greater potential of the proposed architecture in surviving cyber-attacks. A minor problem is noticed in simulating the unidirectional message alert from the SUPERVISOR to the EMS via Twitter message. Under this setup and scenario, the message being sent to the Twitter account may be captured and replaced with false message. Even though the false message would not warn the substation system's operation, there is a great chance that no one would be alerted to come to the substation to address the problem. It is hoped that, in real application of the proposed architecture, the suggested unidirectional fiber optic network would do the intended function properly.

VI. Conclusions

The current period may be appropriately called a cyber-age which has changed every aspect of business operations, factory manufacturing, process operations, and our daily lives in to digital data and cyber bits. The inevitable side effect of this transforming convenience of cyber-age is the cyber threats and attacks whose skills and tactics and targets are not static but constantly evolving. Even with numerous countermeasures supported by government and industry agencies and experts, new threats seem to materialize as soon as old ones are solved or patched. Considering the impact and consequence of the service interruption in a safety-critical application, power grid substation in particular, caused by cyber incidents, a new defensive-architecture based control system is proposed, with expectation that this new defensive architecture would make a networked computer control system cyber-strong and resilient even under compromised situations. The defensive architecture is centered around the diversified redundancy principle and supervised operation with unidirectional communication against malware attacks. The architectural details of the new proposed system are described along with its advantage in surviving cyber-attacks and in overcoming the vulnerability of the existing system. Also detailed is the evaluation process in DeterLab test bed simulation and the lab hardware experimentation, which demonstrates the validity and survival potential of the proposed defensive architecture system under cyber-attacks.

REFERENCES

[1] Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies, October 2009, Department of Homeland Security.

[2] D. Kushner, "The Real Story of Stuxnet," IEEE Spectrum, [Online]. Available: http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet.

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

[4] Charles Kim, "Whitepaper – A Diversified Architecture for Robust and Cyber-Strong Control System," Howard University, 2014. [Internal document.]

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

[6] K. Stouffer, J. Falco and K. Scarfone, "Guide to Industrial Control Systems (ICS) Security," May 2013. [Online]. Available: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r1.pdf.

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

[8] R. HA'AYIN, "Pike Research: Unidirectional Gateways Among Most Promising SCADA Security Technologies," PR News Wire, 13 Sep 2011. [Online]. Available: http://www.prnewswire.com/news-releases/pike-research-unidirectional-gateways-among-most-promising-scada-security-technologies-129710343.html.

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

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

[11] "Trojan-Threat Encyclopedia," Trend Micro USA, November 20, 2014 [Online].

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

[13] "Arduino," [Online]. Available: http://www.arduino.cc/.

AUTHOR PROFILE

Charles Kim is a professor in Electrical Engineering and Computer Science at Howard University, USA. He received Ph.D. degree in Electrical Engineering from Texas A&M University, USA in the year 1989. Prof. Kim's research includes application of physcis of failure to aero, naval, and ground systems of electrical and electronic devices and networks. Also, he has worked for safety and security for safety-critical systems in automotive and energy industrues. Prof. Kim is a senior member of IEEE.