Security by Design: Defense-in-Depth IoT Architecture

Shuangbao (Paul) Wang
paul@computer.org
Columbus State University
Columbus, Georgia

Rose Shumba
shumba@usna.edu
US Naval Academy
Annapolis, Maryland

William Kelly
william.kelly@metonymylabs.com
Metonymy Corporation
Fairfax, Virginia

Abstract - In this paper we propose a defense-in-depth IoT architecture that uses multiple layer security measures involving two security mechanisms in discovering and understanding attack vectors. The advantage is that the impact of failure in any one measure is minimized. The defense-in-depth architecture uses firewalls, demilitarized zones, intrusion detection and prevention systems along with associated security policies. For data acquisition and abstraction, we use multiple-tier data models with REST API at the bottom layer and a system process in extracting, processing and feeding data to the application API.

Using the newly proposed architecture, we are implementing a water treatment SCADA system that has more than 3,000 PLCs. The data acquisition layer uses US Department of Defense developed API to collect data. The defense-in-depth architecture reduces the risk to IoT networks. Initial tests show that the proposed architecture has the advantages of easy connecting various sensors and reducing the risks of cyber intrusions.

Categories and Subject Descriptors

K.5.2 [Legal Aspects of Computing]: *Governmental Issues – Regulation*

General Terms

Security and Privacy – Systems Security – Firewalls; Network Security - Protocols

Keywords

IoT security, SCADA, architecture, smart city, data models

1. INTRODUCTION

The advent of Internet of Things (IoT) brings with the promise of improved livability, workability, and sustainability for millions of people in urban, suburban and rural settings. For individuals, communities and cities, it opens up the opportunity to gather a wealth of new data that drives societal success and quality of life.

Recent Distributed Denial of Service (DDoS) attack shut down the services such as Twitters for hours. It was discovered that Internet cameras contributed the attack. As millions of open network cameras and many more similar IoT devices on the Internet, securing those devices is becoming necessary.

As one of the major categories of IoT systems, Supervisory Control and Data Acquisition (SCADA) is a distributed Industrial Control System (ICS) which enables to monitor and control processes distributed across remote sites. ICSs are typically used in industries such as clean water supply, water treatment plants, electric, oil and gas, transportation, chemical and many other critical infrastructure sectors. SCADA systems are designed to collect data from the field, transfer it to a remote command and control center, perform data abstraction, and visualize the information to the operators and decision makers in real time.

A typical SCADA network consists of the following basic components:

- Sensors
- PLCs/RTUs (Remote Terminal Units)
- Network and communication equipment
- HMI (Human Machine Interface)
- Servers/MTU (Mater Terminal Unit)

Firewalls, Intrusion Detection Systems and Intrusion Prevention Systems (IDS/IPSP and Demilitarized zones (DMZs) are not equipment on traditional SCADA systems.

SCADA networks undergird critical infrastructure, such as electric grids, transportation hubs, and nuclear power plants. They also link to systems containing valuable and sensitive personal information, such as hospitals, schools, and government institutions. A failure in of one of these systems or a cascade of such failures across systems, either in their operations or security, could lead to potentially catastrophic consequences for the population of that region, city and beyond. Yet many of the hardware and software elements used to control, monitor, and connect these systems were not designed with built-in security, while others are outmoded and may not interface with newer technologies. For this reason, every smart and connected cities project must address the security and perform risk analysis [16, 17, 18, 19]. Architecture security by design can make SCADA networks resilient in the face of cybersecurity threats and recover from attacks.

Teams from both private industry and government agencies have developed many innovative technologies to address the security and privacy issues involved in SCADA networks and smart cities [1, 2, 5, 6, 20, 28]. However, due to the complexity of these problems, the problems are hardly solved with the current architecture. A security by design approach and defense-in-depth architecture must be implemented to make SCADA networks free from data breaches.

The National Institute of Standards and Technology (NIST) started a Global Cities Team Challenge in 2013. It has brought together companies, universities, and other organizations to form teams that developed and applied networked technologies [3, 4, 8, 9, 14, 29].

On the data accumulation side, Experience API (xAPI), developed by US Department of Defense (DoD) has proven valuable in congregate data generated from various sensors [7].

The xAPI comes with a data store names LRS, which is a serial database that stores data generated in the SCADA networks. The primary advantage of using xAPI is that devices are connected through xAPI using an HTTP protocol, with which all devices feed data to the LRS database one attribute at a time.

On the data abstraction side, a system process retrieves data from LRS, filter and process and feed to system API for visualization on a dashboard.

The Internet of Things (IoT) reference model (see Figure 1) contains seven layers. For this research, we focus on the architecture and data layers (accumulation and abstraction).

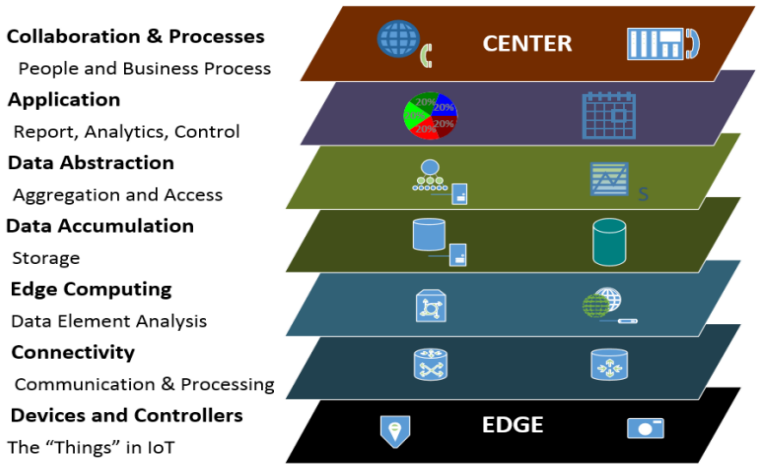

Figure 1: Internet of Things Reference Model

1. SECURE ARCHITECTURE FOR SCADA SYSTEMS

The Internet of Things connects home appliances, sensors, traffic, vehicles, medical aids, smart grids, and industrial automation. The heterogeneous collection of microcontrollers, sensors, data interfaces and networks makes it difficult to setup up a secure SCADA network and to design a database schema for storing the collected data. The study of IoT and SCADA architecture involves how to integrate different technologies and how to interconnect the heterogeneous set of controllers and sensors, whether centralized or distributed.

Representational State Transfer (REST) is an architectural model for uniformly accessing a resource and modifying a resource. It is commonly seen on many web-based APIs that uses JSON over HTTP, though some people propose to use REST without JSON as an IoT protocol in the future.

Zanella proposes the Constrained Application Protocol (CoAP), which is considered more suitable for constrained devices. CoAP supports the REST methods of HTTP GET, PUT, POST, and DELETE. So it can be natively supported by different hosts on the Internet.

Currently most city infrastructure is either not connected at all or connected in a standalone state. Fresh water facilities have used very limited sensors to detect water quality. Water treatment plants are mostly controlled by PLCs, but the data are only accessible at the particular plant. Data are not shared at a city level therefore no feedback or control can be given.

Industrial Control Systems have been widely used in the water treatment systems of cities around the world. The big data and smart cities movements push these systems to go beyond standalone systems. Now many control systems are interconnected to form a SCADA network [10, 11, 12, 13]. This brings opportunities for cities and utilities companies to monitor the water quality and performance of water treatment equipment across a city, region, or even country. As a result, it is critical to study the system architecture necessary for securely transmitting data to the remote databases and securely sending commands to the

distributed PLCs, especially for PLCs that are connected to critical infrastructure such as nuclear power plants, transportation hubs, power grids, and others.

Water SCADA system is composed of sensors, flow meters, pump and value control, pH value and temperature measurements, chemical flow rate control, operator console and servers. Adding firewall, performing risk analysis and vulnerability assessment on those systems are necessary [22, 23, 24, 25].

The SCADA system we are building connects each water treatment facility by collecting information and issuing commands. Each water treatment system gathers data from PLCs, which are connected to various sensors.

1.1 Vulnerabilities in IoT devices

Vulnerabilities on Siemens S7-1200 PLC could allow an attacker with automation network access to execute various unauthorized commands. Using cross-site scripting attacks, an attacker could access Cookies, session variables and APIs that could reveal weak encrypted passwords (such as MD5). Even though Siemens published an update to fix the problem, many PLC implemented in the industrious sites are not able to be updated.

Vulnerabilities in xAPI cold reveal account information over the Internet. As a result, it would be possible for attackers to inject or steal data from the remote unencrypted database.

Many network cameras are not equipped with strong encryptions or with no encryption at all. Once gaining control of the cameras, an attacker can basically do whatever he wants to do.

Figure 2 shows by capturing the packets, we are able to reveal wi-fi network the robot is using, all source code resides on the robot, account information of the owner, and the encryption it used.

We also discovered that the communication was encrypted with MD5, which can be easily decrypted. Using the software update function, malicious code can be

injected to turn this $10,000 robot into a "zombie", which can then be used to launch DDoS attacks when waking up by attackers.

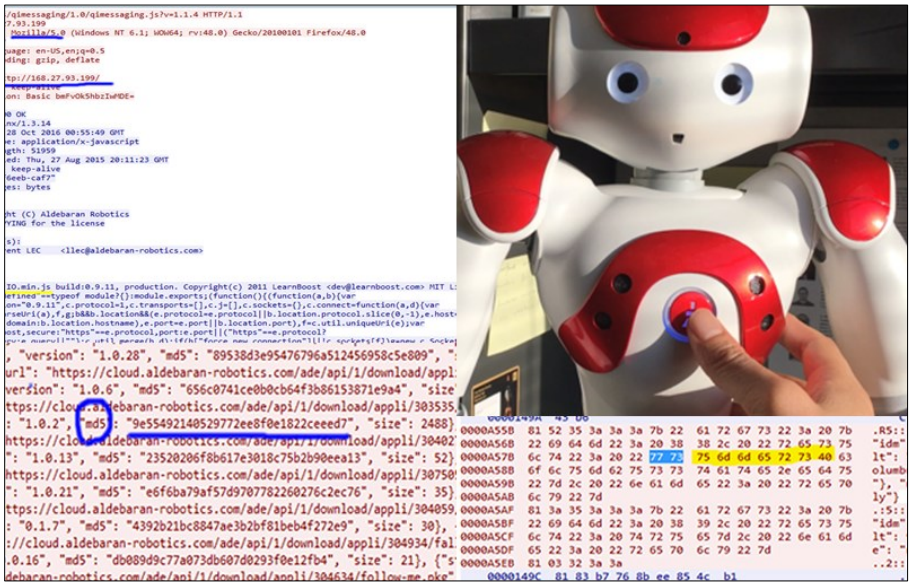

Figure 2: Demonstration of Attacking a Robot

2.2 Security Architecture using Paired Firewalls

SCADA networks and corporate networks should be segregated to enhance security. Using a two-port firewall between the corporate and SCADA networks, security can be improved on condition that the firewall is properly configured.

Establish a DMZ between the corporate and SCADA networks shields the networks from outside world. Creating a DMZ requires that the firewall offer three or more interfaces, one is connected to the corporate network, the second to the SCADA network, and the third to the shared or insecure servers or wireless access points on the DMZ network.

The paired firewall architecture uses a pair of firewalls positioned between the corporate and SCADA networks. Data servers are placed in the DMZ. The advantage of this architecture is the first firewall blocks the arbitrary packets coming

to the SCADA network or servers in the DMZ. The second firewall prevents unwanted traffic from a compromised device from entering into the SCADA network. It also prevents SCADA network traffic from impacting the shared servers in the DMZ.

The new architecture we proposed uses paired firewalls. It has three zones and contains a DMZ. It is a more secure, manageable and segregation architecture for SCADA systems (Figure 3).

Though the paired firewall architecture increased cost and management complexity, it has strong advantages by increasing the security.

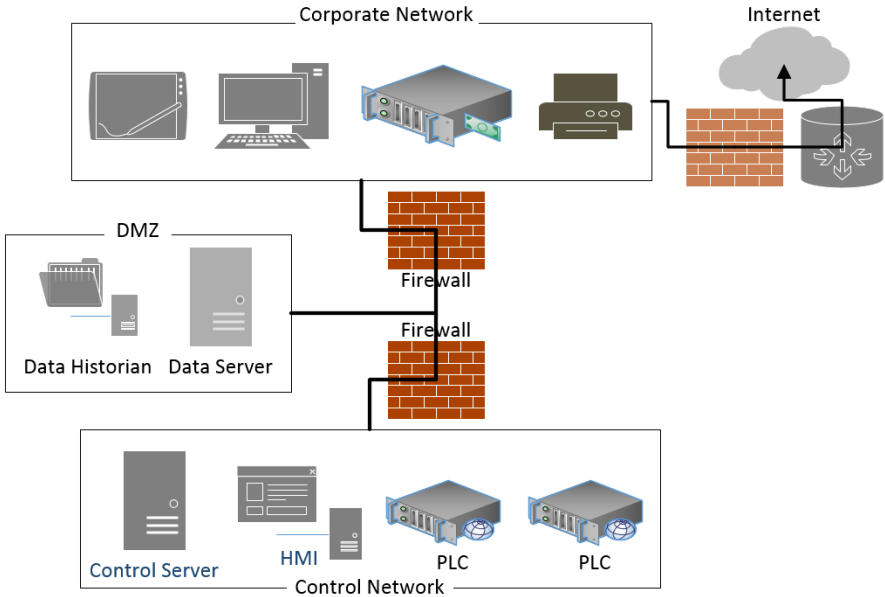

Figure 3: Paired Firewall Architecture

2.3 Defense-in-depth SCADA Architecture

Using firewalls alone cannot adequately protect SCADA networks. A multiple layer architecture involving two or more security mechanisms is a better approach. This is a technique commonly known as defense-in-depth where the impact of a failure in one measure cannot cause failure of the whole system thus minimizes the business services to be interrupted. Defense-in-depth includes the use of two or more firewalls, the creation of DMZs, the employments of IDS/IPS devices along with effective security policies and business operations [26].

- In addition, understanding the following attack vectors is essential:
- Backdoors in applications and in network perimeter
- Vulnerabilities in applied protocols (e.g. open SSL)
- Threats and attacks on field PLCs, smart sensors and other network devices
- Attacks and injections on databases
- Session hijacking using "man in the middle" attacks.
- Phishing and spoofing on privileged accounts
- Attack through supply chain networks.

Our defense-in-depth strategy includes firewalls, the use of demilitarized zones (DMZ) and intrusion detection capabilities throughout the SCADA architecture. The use of several DMZs provides the added security to separate functionalities and access privileges and has proved to be effective in protecting large architectures from being comprised (Figure 4).

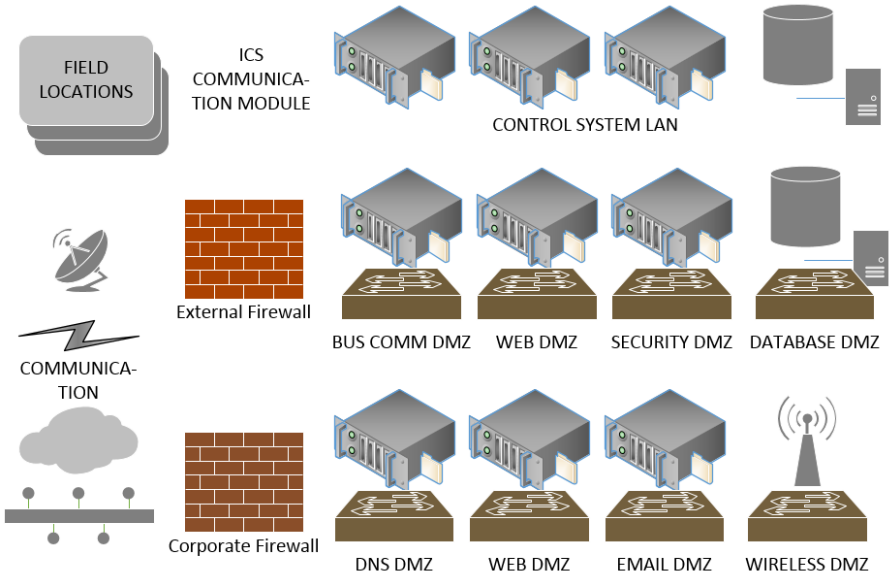

Figure 4: Defense-in-depth SCADA Architecture

2.4 Multi-tier Data Models for Data Acquisition and Abstraction

Developed by the DoD, xAPI is an abstract application interface for storing and retrieving data across different platforms and formats. Unlike relational databases, in which data are inserted into databases in parallel (one row at a time), xAPI technology enforces a consistent data structure for inserting only one attribute at a time. If relational databases are considered parallel, then xAPI databases are serial. The main advantage to use serial databases is its interoperability, allowing it to effectively store data from various platforms or sensors. Data are transmitted from sensors via LAN, Wi-Fi, or cellular wireless connections to a remote database/LRS via xAPI [27].

Since serial databases store one attribute at a time, this makes it a perfect choice for the heterogeneous collection of sensors and control devices in IoT systems. The implementation of such serial databases can be easily achieved with xAPI that is based on REST model and JSON.

Data abstraction was done using a system process that reads data from the serial database, processes and filters data, and sends data to application API which contains a relational database for visualization on a dashboard and for further analysis. Figure 7 shows the process of data abstraction.

2. IMPLEMENTATIONS AND FURTHER DISCUSSIONS

SCADA networks are getting more applications in industries around the world. Threats to SCADA systems and other critical infrastructure are on the rise. One reason for major incidents happened is that SCADA systems lack security by design. Most PLCs are not built with security. Even security considerations have been implemented in the newer models. The overall SCADA system is still vulnerable to cyber intruders.

Figure 5 shows a water treatment SCADA system we are currently implementing. The system contains more than 3,000 PLCs. The original light-and switch control panel is being replaced by a dashboard that displays live data on the remote sites. Command and control can be performed through a web interface that connects to the remote sites.

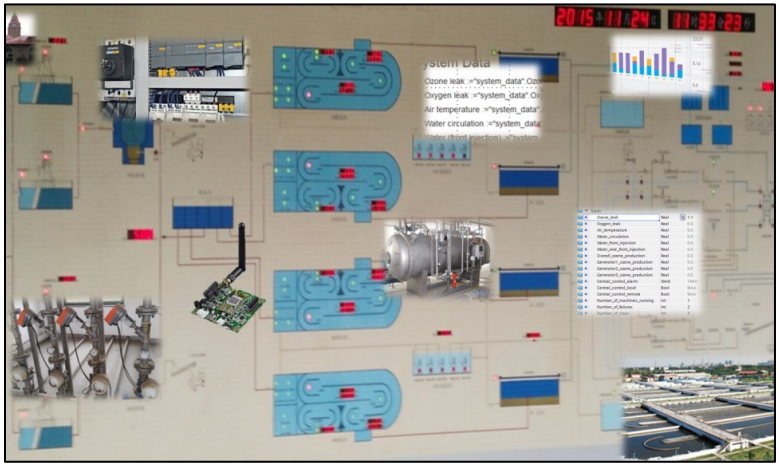

Figure 5: A Water Treatment SCADA System

Using the project as a case study, we add IoT security architecture study and data encryption in our cybersecurity programs. By working on the project, students gain knowledge and hands-on skills in IoT architecture and security.

For data acquisition, authentication and session management are among the weakest aspects of IoT systems. JSON and JavaScript may expose account information on the web from HTTP methods. Using unencrypted protocols, hackers could discover authentication information directly from xAPI configuration, thus penetrating into systems and databases. As a result, strong encryption and a more robust authentication approach must be used, such as the encryption of authentication information using SSL protocol, OAuth 2.0, or smart sensors that have built-in hardware encryption capacities.

REFERENCES

[1] NIST 800-122 (2010). Guide to Protecting the Confidentiality of Personally Identifiable Information (PII), National Institute of Standards and Technology.

[2] Rulz, J. et.al. (2012). A Methodology for the Analysis and Modeling of Security Threats and Attacks for Systems of Embedded Components. 20th Euromicro International Conference on Parallel, Distributed & Network-based Processing. p261-268.

[3] Xu, D. et. al. (2012). Automated Security Test Generation with Formal Threat Models. IEEE Transactions on Dependable & Secure Computing. Vol. 9 Issue 4, p526-540.

[4] NIST (2014). National Initiative for Cybersecurity Education (NICE). National Institute of Standards and Technology.

[5] Mousavian, S., Valenzuela, J. & Wang, J. (2015) A Probabilistic Risk Mitigation Model for Cyber-Attacks to PMU Networks. IEEE Transactions on Power Systems. Vol. 30 Issue 1, p156-165.

[6] Privacy Clearinghouse. (2014). University of Maryland, College Park. Retrieved from https://www.privacyrights.org/data-breach-asc?title=maryland

[7] Baltimore Sun (2014). UMCP reports another cybersecurity breach. Retrieved from http://www.baltimoresun.com/news/maryland/education/blog/bs-md-umd-another-cyberattack-20140320,0,798878.story#ixzz3EAtmElmM

[8] Wang, S. & Ledley, R., Computer Architecture and Security, Wiley, ISBN 978-1-1181-6881-3. January 2013.

[9] Experience Application Program Interface (xAPI). (2015). Advanced Distributed Learning. Retrieved from http://www.adlnet.gov/wp-content/uploads/2013/05/20130521_xAPI_v1.0.0-FINAL-correx.pdf

[10] Cybersecurity for smart city architecture (2015). National Institute of Standard and Technology (NIST). Retrieved from http://nist.gov/cps/cybersec_smartcities.cfm

[11] City Science (2015). Massachusetts Intitute of Technology (MIT). Retrieved from http://cities.media.mit.edu/

[12] Hernan, S. et. al. (2006). Uncover Security Design Flaws Using The STRIDE Approach. Retrieved from https://msdn.microsoft.com/en-us/magazine/cc163519.aspx

[13] Threat Modeling. (2015). Microsoft Corporation. Retrieved from https://msdn.microsoft.com/en-us/library/ff648644.aspx

[14] Wang, S., Kelly, W. & Zhang, J. (2015). Using Novel Video Indexing and Data Analytics Tool to Enhance Interactions in e-Learning. In Proceedings of Association for the Advancement of Computing in Education (AACE). pp. 1919-1927.

[15] Wang, P. & Kelly, W. (2015). Threat Intelligence and Risk. Proc. of Center of Academic Excellence in Cybersecurity Education (CAE), NSA/DHS. in press.

[16] Saitta, P., Larcom, B, & Eddington, M. (2005). Trike v.1 Methodology Document. Retrieved from http://octotrike.org/papers/Trike_v1_Methodology_Document-draft.pdf

[17] Whiteman, B. (2008). Network Risk Assessment Tool (NRAT). IA newsletter, Vol 1. Retrieved from http://iac.dtic.mil/iatac/download/Vol11_No1.pdf

[18] PASTA. (2015). Process for Attack Simulation and Threat Analysis Risk-Centric Threat Modeling. OWASP. Retrieved from https://www.owasp.org/images/a/aa/AppSecEU2012_PASTA.pdf

[19] Wang, P., Ali, A., Zhang, J., and Kelly, W. (2014). inVideo - A Novel Big Data Analytics Tool for Video Data Analytics and Its Use in Enhancing Interactions in Cybersecurity Online Education. WIT Transactions on International conference on Communication Technology and Application. Vol. 60. pp.321-328.

[20] Hutchins, E. M., Clopperty, M. J. & Amin, R. M. (2010). Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains. Retrieved from http://papers.rohanamin.com/?p=15

[21] WASC Threat Classification v2.0. (2015). Web Application Consortium. Retrieved from http://projects.webappsec.org/w/page/13246978/Threat Classification

[22] FIRST. (2015). Common Vulnerability Score System v3.0. Retrieved from https://www.first.org/cvss/cvss-guide

[23] OWASP. (2015). Application Threat Modeling. The Open Web Application Security Project. Retrieved from https://www.owasp.org/index.php/Application_Threat_Modeling

[24] Wang, S. and Zhang, J. (2014). A Video Data Search Engine for Cyber-Physical Traffic and Security Monitoring Systems. Proc. of IEEE/ACM Fourth International Conference on Cyber-Physical Systems. pp. 225-226.

[25] Wang, P.; Ai, A.; Kelly, W. (2015). Data Security and Threat Modeling for Smart City Infrastructure. Proc. of IEEE Cyber Security of Smart Cities, Industrial Control System and Communications. pp.1-6.

[26] Wang, P. & Kelly, W. (2015). A Novel Threat Analysis and Risk Mitigation Approach to Prevent Cyber Intrusions. Journal of Colloquium for Information system Security Education (CISSE). Vol. 3, Issue 1, pp. 157-174.

[27] Michael Koster. (2016). Data Models for the Internet of Things. Retrieved from http://iot-datamodels.blogspot.com/.

[28] Department of Energy. (2016). 21 Steps to Improve Cyber Security of SCADA Networks. Retrieved from http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/21_Steps_-_SCADA.pdf.

[29] NIST Special Publication 800-82 Revision 2 (2015). Guide to Industrial control Systems (ICS) Security. National Institute of Standards and Technology.