ADAPTING SCADA SYSTEMS TO CLOUD COMPUTING ENVIRONMENT

Zhixiong Chen and Donovan Evan
Math and CIS, Mercy College, Dobbs Ferry, New York, NY 10522, U.S.A.

Keywords: Cloud computing, Supervisory control.

Abstract. Supervisory Control and Data Acquisition (SCADA) systems have existed for over 50 years. Yet, they are still widely used in national critical infrastructures like New York Metro transportation system, NY waterway control systems and power grid. This paper examines the evolution of SCADA systems from closed SCADA systems to open networked SCADA systems and discusses issues adapting SCADA systems into cloud computing paradigm. We propose a framework that secures SCADA systems under cloud environment. It provides reasonable assurance of such adaptation and migration. Finally, we apply it to NY Metro North Subway and Rail Transportation system.

1 INTRODUCTION

Supervisory Control and Data Acquisition or SCADA refers to any systems and networks that monitor, manage, and control automation, production and distribution (SCADA and CS).

SCADA systems are widely used in nations' critical infrastructure such as transportation, telecommunications, energy, waste and water treatment, and manufacturing (SCADA).

Securing SCADA systems is a national priority because disruption of them can have significant consequences for public health and safety (PDD 63).

When SCADA systems are set to be isolated standalone control systems, security concerns are more on the physical access control and operators. When SCADA systems are networked and/or hooked into internet, the security concerns are shifted to more or less the same as we do to network security and information systems. A whole range of security issues such as access control, business continuity and disaster recovery planning, security governance and risk management, law regulations and compliance, operations security; environmental security, security architecture and design, and telecommunications and network security need to be addressed (Krutz, 2006; Chen and Yoon, 2010).

For the last several years, cloud computing is moving from industry to academia (instead of the other direction like many classical cases) and is making leap in IT evolution. It is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction (NIST). With on-demand self-service, broad network access, resource pooling, rapid elasticity and measured services, cloud computing increases greatly productivity and efficiency (NIST). At the same time, security is a great concern (Cloud Security Alliance, 2009). Many research papers and frameworks are devoted to this area (for example, see (Krutz, 2006; NIST; Cloud Security Alliance, 2009; Chen and Yoon, 2010; http://en.wikipedia.org/; Forrest, 2009; NIST, 2010; OSAG). Cloud Security Alliance identifies thirteen (13) domains that need to be covered in securing cloud computing environment (Krutz, 2006) while Chen et al discusses compliances for services deployment models thoroughly (Chen and Yoon, 2010).

Migrating networked SCADA systems to a cloud environment, either a private cloud or a public cloud, is sure a path for better data sharing, data managing and quick decision making. But, security and compliance, especially for public cloud are certainly big concerns. As we see recently that a window computer worm, stuxnet and its variants are found to target industrial systems and their payload to PLC in SCADA systems (http://en.wikipedia.org/). It is a very sophisticated attack to SCADA systems. We can only expect that a big

Chen Z. and Evan D..
ADAPTING SCADA SYSTEMS TO CLOUD COMPUTING ENVIRONMENT.
DOI: 10.5220/0003614705590563
In *Proceedings of the 13th International Conference on Enterprise Information Systems* (IAST-2011), pages 559-563
ISBN: 978-989-8425-55-3

organization or even government agency can have such capabilities.

In this paper, we will address these issues from classical SCADA systems to cloud environment. In section 2, we examine the evolution of SCADA systems while in section 3, after summarizing cloud computing services deployment models, we discuss the feasibility of moving networked SCADA systems to cloud environment, from private cloud, community cloud to public cloud. In section 4, we list specific security and compliance issues facing migrating SCADA systems into cloud and propose a framework of securing SCADA systems. We use NY Metro North Subway and Rail systems as an example to demonstrate our work. The final section is devoted to discussion and further research and field work.

2 EVOLUTION OF SCADA SYSTEMS

Traditionally, Electrical Engineers consider SCADA systems as control systems (CS). A typical SCADA system architecture can be demonstrated by Figure 1 in which a SCADA host uses Human Machine Interface (HMI) to connect to several Remote Terminal Units (RTUs) or Programmable Logic Controllers (PLCs) and to acquire data and to make controls. RTUs and PLCs are in closed loop control to field elements such as sensors, valves, pumps, switched and motors via EIA232 and EIA485.

Human operators control supervisory functions and monitor them. The monitoring devices continually update data, which enable operators to manage daily operations locally and remotely as well. HMI systems have evolved from light indication panels and analog gauges to computerize graphical display with real time indication and response features.

Communication medium is more on copper line due to the unreliability of earlier radio systems and the high cost of ISDN lines. Communication protocols are mostly in the application layer and most of them are still proprietary like MODBUS from Modicon. The trend is that these proprietary protocols are moving toward open and standardized protocols, for example, Profibus from Siemens, Device Net from Allen Bradley, DNP3 and subsequently IEC61850 from EPRI, and IEEE 60870.

Computer scientists consider SCADA systems as connected IT systems. A typical networked SCADA system can be depicted by Figure 2 in which several SCADA hosts uses HMI to connect Master Terminal Units (MTU) that serves as a basic central control station (BCCS). The BCCS hooks with controllers like RTUs and PLCs securely via wireless network, Switched Public Telephone Network or Internet. These controllers link to field elements.

The efforts of moving standalone SCADA systems to networked SCADA systems represent an evolution path of SCADA systems when they were first appeared about fifty years ago.

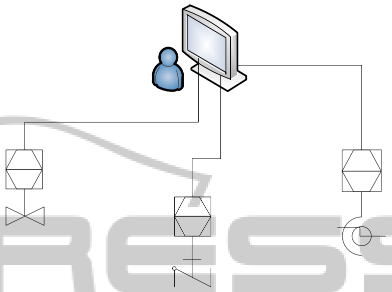

Figure 1: A typical Standalone SCADA System.

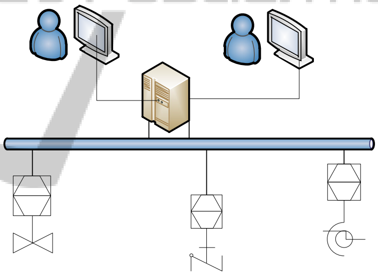

Figure 2: A typical Networked SCADA System.

3 ADAPTING SCADA SYSTEMS TO CLOUD COMPUTING

The notion of moving SCADA systems into cloud computing is quite controversial and eye catching. Some researchers believe it will benefit greatly for the next generation SCADA systems such as smart grid, renewable energy (Vyatkin, 2010; Gustavsson and Ståhl, 2010; Geberslassie and Bitzerl, 2010) and the virtualization concept in cloud is actually enhancing security (Communication in ACM) while others believe the virtualization is overkill, especially when defending malware such as rootkit (Bratus, 2010).

In our survey of NY Metro North Subway and Rail SCADA system (Figure 3 and 4), while it is wary about the idea of opening its SCADA system to a cloud, especially about to a public cloud, it believes it will benefit if it adopts some of the typical cloud features or characteristics like self-configuration, broad network access and resource pooling.

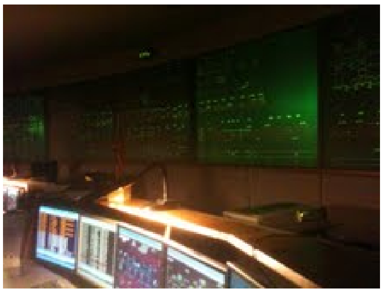

Figure 3: Control Room.

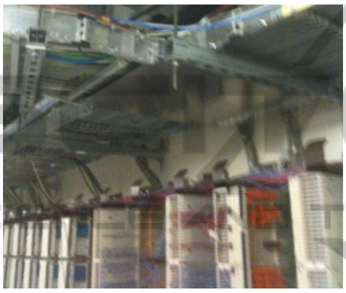

Figure 4: Communication Room.

For example, virtualization can help mass configuration if it updates its out-dated controllers to more standard network enabled ones with more processing power and memory. Another example is using IP cameras to monitor remote controllers and field elements can be done in a private cloud environment. The surveillance system can be independent from the existing SCADA system or be a part of SCADA system that can trigger a sequence of control actions when undesired events like intruders, fire alarm, and power shortage are detected. Processing, protecting and preserving these high volume video streaming data is an ideal candidate for cloud computing.

Because of security concerns in most times is triumph over cost saving due to the nature of SCADA systems, we do not see the possibility of moving SCADA to a public cloud in the near future unless some special arrangements or dramatic security technology advancement. Like many big trading companies that do not use a public cloud but shift to a private cloud internally, SCADA systems can adapt to a private cloud or even a community cloud that shares the same concerns. As we know, cloud computing is basically a collection of net centric technologies. A private cloud can shield the notion of open SCADA systems to public although it is not absolutely true. At the same time, SCADA systems in the cloud can share the computing resources needed, sharing data acquired from field controllers so that decision makers can have accurate and near real time data.

We need to emphasize that a private cloud is not sharing controls while sharing data. Technically, sharing data can be done using various mechanisms. One non-intrusive mechanism is to capture image displayed in an operator screen inside a SCADA host. This will make the alteration of data during transmission much harder. It addresses more data integrity than confidentiality. So the adaptation should move in a careful staging process.

Another area is to provide redundancy resources. SCADA systems controllers can stretch over a large geography area. They are vulnerable to terrorism, vandalism or lost of system controls. System reliability is of the utmost importance; therefore redundancy is prevalent throughout the system. The Control center and each RTU have a dedicated UPS system, redundant communication lines, and servers. Cloud network would solve many of these issues.

4 SECURITY AND COMPLIANCE OF SCADA SYSTEMS IN CLOUD

In a keynote address to the National Science Foundation workshop on Critical Infrastructure Protection for SCADA & IT, Dr. Arden Bement listed several incidents to illustrate the vulnerability of SCADA systems (NSF Workshop, 2003). He dismissed the notion of “Obscurity” if we think SCADA systems are highly customized, highly technical, and therefore the guys in the black hats won't be able to figure them out in addition to the fact that 60 to 70 percent of all industrial security breaches are carried out by someone on the inside.

NSA lists a checklist on securing SCADA and CS (Control Systems): Develop a Security Policy; Establish Physical Security; Lockdown Perimeter Security; Enable Existing Security Features; Secure Operational Traffic; Secure Management Traffic; Manage the CS Configuration; Eliminate Security Shortfalls; Continuous Security Training; and Perform Security Audits Systems (SCADA and CS).

Developing a proper security policy set a foundation for securing SCADA systems and its CS assets. It defines and places controls in various stages. With security policy in place, proper enforcement plays crucial roles in securing SCADA systems. For example, strict access control to SCADA should be periodically reviewed. Cut off unnecessary connection to outside is essential.

One of the major issues with SCADA systems are legacy devices and proprietary protocols that are still in use. Although many of existing SCADA equipments is quiet reliable, their support is more and more difficulty due to the change in manufacturing and the advance in technology. In addition, many manufacturers have stopped supporting these equipments that use proprietary protocols. Therefore many system managers are anxious to upgrade their SCADA systems. On one hand, it provides an opportunity for better data translation, data propagation and data protection when companies start to upgrade its devices in SCADA system to more standardized ones. On the other hand, it also poses great potential problems when legacy devices are used with these newer devices. Not only are data translation and data propagation not supported, performance and reliability will suffer as well. System administrators often fail to conduct proper risk analysis of their current system and the implementation of any new technology. Development of platforms that interact with legacy systems and the modern SCADA network help to create the synergy necessary to achieve an efficient and reliable platform that has the ability to give the security, reliability and adaptability.

When moving networked SCADA systems into Cloud, we also need to develop checklists for auditing that will provide a level of confidence of doing things right and doing right things, just like we did when we moved standalone SCADA systems to networked SCADA systems.

Progress in the area of standardization is best achieved by external organizations such as International Standards Organization (ISO), International Federations of Information Processing Societies (IFIPS), the Institute for Electric and Electronic Engineers (IEEE), the International Communications Associations (ICA), and other well respected and recognized groups (Selig, 2003).

In the utilization of cloud services, the assumption should be a predication that such cloud services should show a level of reliable and security. The goal of the designer should be to create a level of security that will enable the system to remain secure if any part of the system is compromised.

Some of the feature needed to create a more secure SCADA cloud system can be summarized in the table 1.

5 DISCUSSION

Moving networked SCADA systems to a public cloud has many unanswered questions and poses many security challenging. It is often controversial. It is evident when we approached NY Metro North Rail system. But, private cloud and even community cloud is more acceptable. The project also assesses existing SCADA equipments that are amazingly

Table 1: Securing Cloud SCADA Systems.

Auditing	Internal auditing External auditing
Data encryption	VPN PKI Systems
Physical Security	Facilities People Environment equipment
Software Security	Trustworthy Conformant Predictability
Business Continuity and Disaster Recovery	Continuity Planning Identify Critical Business Function Establish Recovery Time Objective
Network Security	Establishing a Network Security Management Team Transmission Control Connection Control
Quality of service	Measurable metrics
Framework	COSO COBIT ISO27001

reliable although outdated. It is in the process of updating these equipments.

Recently, we see renewed interests in SCADA systems. Not only are SCADA systems still used in our national critical infrastructures such as power grid, railway systems, gas pipelines and nuclear power plants, but also the movement from isolated systems to more open systems and lack of skilled professionals. Research and training are both important. Both NSA (National Security Agency) and DHS (Department of Homeland Security) have looked into our national SCADA systems, its vulnerability and weakness as well as protection mechanisms ((SCADA and CS; Testimony of Deputy Under Secretary Philip Reitinger; Securing Industrial Control Systems in the Chemical Sector, 2011), for example).

In summary, we should pay more attentions to SCADA systems and the trend of upgrading. Proper risk assessment should be done. Cloud computing has huge potential in IT services. Incorporating both should be able to deliver more efficient control systems.

REFERENCES

Securing Supervisory Control and Data Acquisition (SCADA) and Control Systems (CS), http://www.nsa.gov/ia/_files/factsheets/scada_factsheet.pdf

SCADA at http://en.wikipedia.org/wiki/SCADA

Protecting America's Critical Infrastructures: PDD 63 http://www.justice.gov/criminal/cybercrime/white_pr.htm

Krutz R., Securing SCADA Systems, *Wiely Publishing Inc*, 2006

NIST Definition of Cloud Computing v15, http://csrc.nist.gov/groups/SNS/cloud-computing/cloud-def-v15.doc

Security Guidance for Critical Areas of Focus in Cloud Computing V2.1, by Cloud Security Alliance, December 2009. https://cloudsecurityalliance.org/csaguide.pdf

Chen, Z. and Yoon, J.: IT Auditing to Assure a Secure Cloud Computing. The proceedings of the *6th IEEE World Congress on Services*, July 5-10, 2010, Miami, Florida, USA, 253-259

http://en.wikipedia.org/wiki/Stuxnet for general description

Will Forrest, Clearing the Air on Cloud Computing, Discussion *Document from McKinsey and Company*, March 2009

NIST Presentation on Effectively and Securely Using the Cloud Computing Paradigm v26, accessed on 4/15/2010, http://csrc.nist.gov/groups/SNS/cloud-computing/cloud-computing-v26.ppt

Open Security Architecture Group http://www.opensecurityarchitecture.org/cms/library/patternlandscape/251-pattern-cloud-computing

Vyatkin, V., et al, Toward Digital Ecologies: Intelligent Agent Networks Controlling Interdependent Infrastructures, *1st IEEE Conference on Smart Grid Communications*, Gaithersburg, October, 2010

Gustavsson, R.; Ståhl, B.; The empowered user - The critical interface to critical infrastructures, the *5th International Conference on Critical Infrastructure (CRIS),* 2010

Geberslassie, M.; Bitzer, B.; Future SCADA systems for decentralized distribution systems, the *45th International Universities Power Engineering Conference (UPEC)*, 2010

Communication in ACM, Virtualization is good for security

Bratus, S., Locasto M., Ramaswamy, A. and Smith S.;VM-based security overkill: a lament for applied systems security research, Proceedings of the *2010 workshop on New security paradigms*, 51-60, 2010

The NSF Workshop on Critical Infrastructure Protection for SCADA & IT in Dr., Director - National Institute of Standards & Technology, October 20, 2003, http://www.nist.gov/director/speeches/bement_102003.cfm

Selig, Gad J. "Strategic Planning for Information Resource Management A Multinational Perspective" *UMI Research Press Ann Arbor*, Michigan 2003

Testimony of Deputy Under Secretary Philip Reitinger, National Protection and Programs Directorate, Before the United States House Committee on Homeland Security Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies, "Examining the Cyber Threat to Critical Infrastructure and the American Economy" (http://www.dhs.gov/ynews/testimony/testimony_1300283858976.shtm)

Securing Industrial Control Systems in the Chemical Sector, Roadmap Awareness Campaign – A Case For Action, Developed by the Chemical Sector Coordinating Council in partnership with the U.S. Department of Homeland Security, April, 2011 (http://www.dhs.gov/xlibrary/assets/oip-chemsec-case-for-action-042011.pdf). Note, DHS has many relevant documents related to the SCADA systems.