Distributed Monitoring: A Framework for Securing Data Acquisition

Matthew Brundage[†]
Anastasia Mavridou[†]
James Johnson[†]
Peter J. Hawrylak[†]
Mauricio Papa[†]
[†]*The University of Tulsa, Tulsa, OK, USA*

ABSTRACT
SCADA systems monitor and control many critical installations around the world, interpreting information gathered from a multitude of resources to drive physical processes to a desired state. In order for the system to react correctly, the data it collects from sensors must be reliable, accurate, and timely, regardless of distance and environmental conditions. This chapter presents a framework for secure data acquisition in SCADA systems using a distributed monitoring solution. An overview of the framework is followed by a detailed description of a monitoring system designed specifically to improve the security posture and act as a first step towards more intelligent tools and operations. The architecture of the Smart Grid is used to analyze and evaluate benefits that the proposed monitoring system can provide. Finally, the effects and use of Radio Frequency Identification (RFID) and ZigBee as data acquisition platforms are discussed in the context of the proposed solution.

INTRODUCTION
Supervisory Control and Data Acquisition (SCADA) systems (NCS, 2004) form the backbone of industries in the areas of electric power, oil and gas, water, and rail transportation. They have been identified by the EU Commission and the U.S. Department of Homeland Security as a core component of most critical infrastructures (Brunner, & Suter, 2008). SCADA systems provide real-time centralized monitoring and control of industrial processes through a combined use of data acquisition and transmission systems and Human-Machine Interfaces (HMIs). In the past, SCADA systems were considered to be secure due to the use of proprietary equipment and software as well as the limited network connectivity and isolation of these systems. However, during recent years, continued SCADA modernization and increased interconnection have resulted in a transition from closed, isolated networks to open, IP-based networks. Therefore SCADA systems are now considered to be part of the cyber infrastructure (DHS & DoE, 2007). The increased interconnection has made SCADA systems more vulnerable to attacks and has introduced new security risks. As a result, there is a pressing need to mitigate these risks.

Currently, in industry, there are several SCADA protocols in use. In the electric sector, the most popular are the International Electrotechnical Commission (IEC) 60870-5-101 (IEC, 2003), commonly referred to as 101, and the Distributed Network Protocol version 3 (DNP3) (Curtis, 2005). IEC is also developing 61850 to provide guidelines for the secure automation and operation of electrical substations. Security in SCADA implementations is a major concern because many SCADA protocols in use today are still operating in unauthenticated clear text. While there is a significant effort to enhance SCADA protocols with security functionality, for example the DNP3 SA (secure authentication) (Gilchrist, 2008), the

majority of systems in the industry sector still use clear text. As a result, in order to enhance the security of SCADA systems and detect any suspicious behavior, SCADA communication networks need to be monitored to provide operators with accurate and timely information about the network devices and their interactions. In particular, a distributed monitoring system will be able to verify that the incoming information is accurate, as well as provide a foundation to support development of more powerful tools such as intrusion detection systems and packet filtering components.

This chapter uses the Smart Grid domain and relevant components in the energy sector to illustrate security concerns in SCADA systems. Although utilities in the electric sector require 24x7 availability, they may not be able to recover quickly and efficiently from all security breaches. Thus, a cyber-attack in this sector can have destructive results. Such an attack on SCADA systems located in the power grid can have a significant impact in the functionality of the grid. In fact, the massive North East Blackout has been linked to the propagation of the MSBlaster worm in 2003 (Verton, 2003; CERT, 2003). Also, the recently discovered W32.Stuxnet rootkit (Falliere, Murchu, & Chie, 2011) is an example of malware targeting Industrial Control Systems (ICS). Falliere (2010) notes that, "Stuxnet has the ability to take advantage of the programming software to also upload its own code to the PLC in an industrial control system that is typically monitored by SCADA systems."

In particular, this chapter contributes a recommended security practice of a monitoring structure for the purpose of improving SCADA security. The proposed distributed monitoring system addresses the important issue of secure data acquisition. This will provide system operators with the information needed for (i) a more intelligent response to incoming information and (ii) increased awareness of possible malicious activity in an environment outside of the control of the SCADA system. The Smart Grid is used as a case study to demonstrate the benefits such a distributed monitoring system could provide.

BACKGROUND

SCADA systems and their communications are currently at a critical point in time, as cyber-attacks become more common and these systems are becoming increasingly interconnected (Craig, Mortensen & Dagle, 2008). A brief overview of the security risks, standards, encryption and authentication, and functionality of the systems will be given.

SCADA Systems

SCADA systems (NCS, 2004) are used to monitor and control critical infrastructures such as energy, oil and gas, water, transportation, and telecommunications. The main components of a SCADA system are:

- Data field devices such as Remote Terminal Units (RTUs) and Programmable Logic Controllers (PLCs) that interface with local sensors and actuators
- The communication network between the SCADA master and the field devices (slaves).
- The SCADA master station located in the control center
- The Human Machine Interface (HMI) devices

Figure 1. SCADA system components

system availability. In addition, tools using data collected by the monitoring system can mitigate overall risks and improve the security posture of the environment.

REFERENCES

ANSI. (2007). *TR99.00.01-2007, Security for Industrial Automation and Control Systems, Part 1: Terminology, Concepts and Models.*

ANSI/ISA. (2007). *TR99.00.01-2007, Security Technologies for Industrial Automation and Control Systems.*

ANSI/ISA. (2009). *TR99.02.01-2009, Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control Systems Security Program.*

Baumeister, T. (2010). *Literature review on smart grid cyber security.* University of Hawaii, Department of Information and Computer Sciences. Retrieved January 23, 2012, from http://csdl.ics.hawaii.edu/techreports/10-11/10-11.pdf

Becker, E., Metsis, V., Arora, R., Vinjumur, J., Xu, Y., & Makedon, F. (2009). SmartDrawer: RFID-based smart medicine drawer for assistive environments. *2nd International Conference on PErvasive Technologies Related to Assistive Environments (PETRA '09).* New York, NY.

Berthier, R., Sanders, W., & Khurana, H. (2010). Intrusion Detection for Advanced Metering Infrastructures: Requirements and Architectural Directions. *First IEEE International Conference on Smart Grid Communications (SmartGridComm)*, (pp. 350-355). Gaithersburg, MD.

Brownfield, M., Gupta, Y., & Davis, N. (2005). Wireless sensor network denial of sleep attack. *Sixth Annual IEEE Information Assurance Workshop* (pp. 356-364). West Point, NY: IEEE.

Brunner, E., & Suter, M. (2008). International CIIP Handbook 2008/2009 An Inventory of 25 National and 7 Internation Critical Information Infrastructure Protection Policies. Zurich, Switzerland: ETH.

Buennemeyer, T., Jacoby, G., Chiang, W., Marchany, R., & Tront, J. (2006). Battery-Sensing Intrusion Protection System. In *2006 IEEE Information Assurance Workshop* (pp. 176-183).

Bustillo, M. (2010, July 23). Wal-Mart Radio Tags to Track Clothing. *Wall Street Journal*. Retrieved February 18, 2011, from http://online.wsj.com/article/SB10001424052748704421304575383213061198090.html

Cardenas, A. A., Roosta, T., & Sastry, S. (2009). Rethinking security properties, threat models, and the design space in sensor networks: A case study in SCADA systems. *Ad Hoc Networks, 7*(8), 1434-1447.

CERT. (2003). *Advisory CA-2003-20 W32/Blaster worm.* Carnegie Mellon University's Computer Emergency Response Team. Retrieved January 23, 2012, from http://www.cert.org/advisories/CA-2003-20.html

Chen, M., Gonzalez, S., Leung, V., Zhang, Q., & Li, M. (2010). A 2G-RFID-based e-healthcare system. *IEEE Wireless Communications, 17*(1), 37-43.

Craig, P., Mortensen, J., & Dagle, J. (2008). *Metrics for the National SCADA Test Bed Program, PNNL-18-31*. Richland, WA: Pacific Northwest National Laboratory.

Curtis, K. (2005). *A DNP3 Protocol Primer (Revision A)*. Retrieved May 25, 2011, from http://www.dnp.org/AboutUs/DNP3%20Primer%20Rev%20A.pdf

DHS, & DoE. (2007). *Energy: Critical Infrastructure and Key Resources, Sector-Specific Plan as input to the National Infrastructure Protection Plan.* Department of Energy. Retrieved January 23, 2012, from http://energy.gov/oe/downloads/energy-critical-infrastructure-and-key-resources-sector-specific-plan-input-national

Dondossola, G., Deconinck, G., Garrone, F., & Beitollahi, H. (2009). Testbeds for Assessing Critical Scenarios in Power Control Systems. In R. Setola, & S. Geretshuber (Eds.), *Critical Information Infrastructure Security, Lecture Notes in Computer Science* (Vol. 5508, pp. 223-234). Springer Berlin / Heidelberg.

Emond, J. P. (2008). Resolution and Integration of HF and UHF. In S. B. Miles, S. E. Sarma, & J. R. Williams (Eds.), *RFID Technology and Applications* (pp. 144-156). New York: Cambridge University Press.

EPCglobal. (2008). *EPC™ Radio-Frequency Identity Protocols Class-1 Generation-2 UHF RFID Protocol for Communications at 860 MHz - 960 MHz Version 1.2.0.* EPCglobal, Inc.

Falliere, N. (2010). *Stuxnet Introduces the First Known Rootkit for Industrial Control Systems*. Symantec Official Blog. Retrieved September 5, 2011, from Symantec Official Blog: http://www.symantec.com/connect/blogs/stuxnet-introduces-first-known-rootkit-scada-devices

Falliere, N., Murchu, L., & Chie, E. (2011). *W32.Stuxnet Dossier Version 1.4*. Retrieved September 5, 2011, from Symantec Security Response: http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf

Farahani, S. (2008). *ZigBee Wireless Networks and Transceivers.* Oxford, UK: Elsevier Ltd.

Farhangi, H. (2010). The path of the smart grid. *IEEE Power and Energy Magazine, 8*(1), 18-28.

FERC. (2009). *Smart Grid Policy*. Retrieved January 20, 2012, from Pederal Energy Regulatory Commission: http://www.ferc.gov/whats-new/comm-meet/2009/071609/E-3.pdf

Gilchrist, G. (2008). Secure authentication for DNP3. *IEEE Power and Energy Society General Meeting - Conversion and Delivery of Electrical Energy in the 21st Century*, 1-3.

Gungor, V. C., Sahin, D., Kocak, T., Ergut, S., Buccella, C., Cecati, C., & Hancke, G. P. (2011). Smart Grid Technologies: Communication Technologies and Standards. *IEEE Transactions on Industrial Informatics, 7*(4), 529-539.

Hamoud, G., Chen, R., & Bradley, I. (2003). Risk Assessment of Power Systems SCADA. *IEEE Power Engineering Society General Meeting.*

Hawrylak, P. J., & Mickle, M. H. (2009). EPC Gen-2 standard for RFID. In Y. Zhang, L. T. Yang, & J. Chen (Eds.), *RFID and sensor networks: Architectures, protocols, security and integrations* (pp. 97-124). Boca Raton, FL: Taylor & Francis Group, CRC Press.

Hawrylak, P. J., Cain, J. T., & Mickle, M. H. (2008). RFID Tags. In L. Yan, Y. Zhang, L. T. Yang, & H. Ning (Eds.), *The Internet of Things: from RFID to Pervasive Networked Systems* (pp. 1-32). Boca Raton, FL: Auerbach Publications, Taylor & Francis Group.

Hawrylak, P. J., Ogirala, A., Norman, B. A., Rajgopal, J., & Mickle, M. H. (2011). Enabling Real-Time Management and Visibility with RFID. In A. Kolker, & P. Story (Eds.), *Management Engineering for Effective Healthcare Delivery Principles and Applications* (pp. 172-190). Hershey, PA: IGI Global.

Hoque, E., Dickerson, R. F., & Stankovic, J. A. (2010). Monitoring body positions and movements during sleep using WISPs. *Wireless Health*, (pp. 44-53). New York, NY.

IEC. (2003). International Standard IEC 60870-5-101. Second Edition,. *Telecontrol equipment and systems - Part 5-101: Transmission protocols - Companion standard for basic telecontrol tasks*.

IEC. (2011). IEC/TS 62351: Security. Retrieved October 1, 2011, from International Electrotechnical Commission Web site: http://www.iec.ch/smargrid/standards

IEEE. (1992). *IEEE Recommended Practice for Master/Remote Supervisory Control and Data Acquisition (SCADA) Communications.*

IEEE. (2000). *IEEE Recommended Practice for Data Communications Between Remote Terminal Units and Intelligent Electronic Devices in a Substation.*

IEEE. (2006). *802.15.4-2006 Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (LR-WPANS).* Retrieved from IEEE 802.15 WPAN TG4: http://www.ieee802.org/15/pub/TG4.html

IEEE. (2007). *IEEE Recommended Practice for SCADA and Automation Systems.*

Igure, V., Laughter, S., & Williams, R. (2006). Security issues in SCADA networks. *Computers and Security, 25*(7), 498-506.

ISO. (2009). *ISO/IES 18000-7 Information technology -- Radio frequency identification for item management -- Part 7: Parameters for active air interface communications at 433 MHz.*

ISO. (2010). *ISO/IEC 18000-6: 2010 FDIS Information technology -- Radio frequency identification for item management -- Part 6: Parameters for air interface communications at 860 MHz to 960 MHz.*

Jara, A. J., Zamora, M. A., & Skarmeta, A. F. (2011). An internet of things---based personal device for diabetes therapy management in ambient assisted living (AAL). *Personal Ubiquitous Computing, 15*(4), 431-440.

Kanabar, M., & Sidhu, T. (2011). Performance of IEC 61850-9-2 Process Bus and Corrective Measure for Digital Relaying. *IEEE Transactions on Power Delivery, 26*(2), 725-735.

Khurana, H., Hadley, M., Lu, N., & Frincke, D. (2010). Smart-Grid Security Issues. *IEEE Security & Privacy, 8*(1), 81-85.

Louthan, G., Hardwicke, P., Hawrylak, P., & Hale, J. (2011). *Toward Hybrid Attack Dependency Graphs.* Paper presented at the 7th Annual Cyber Security and Information Intelligence Research Workshop, Oak Ridge.

Massoud Amin, S., & Wollenberg, B. (2005). Toward a smart grid: power delivery for the 21st century. *IEEE Power and Energy Magazine, 3*(5), 34-41.

Mavridou, A., & Papa, M. (2011). A Situational Awareness Architecture for the Smart Grid. *7th International Conference in Global Security Safety and Sustainability (ICGS3).* Thessaloniki, Greece.

McDaniel, P., & McLaughlin, S. (2009). Security and Privacy Challenges in the Smart Grid. *IEEE Security & Privacy, 7*(3), 75-77.

NCS. (2004). *Supervisory Control and Data Acquisition (SCADA) Systems, Technical Information Bulletin NCS TIB 04-1.* Arlington, VA.

NERC. (2011). *Reliability Standards for the Bulk Electric Systems of North America.* Retrieved January 23, 2012, from North American Electric Reliability Corporation: http://www.nerc.com/docs/standards/rs/Reliability_Standards_Complete_Set.pdf

NETL. (2008). *Advanced Metering Infrastructure.* Retrieved January 23, 2012, from http://www.netl.doe.gov/smartgrid/referenceshelf/whitepapers/AMI%20White%20paper%20final%20021108%20%282%29%20APPROVED_2008_02_12.pdf

NIST. (2010). *NISTIR 7628, Guidelines for Smart Grid Cyber Security.* National Institute of Standards and Technology.

Oman, P., Schweitzer III, E., & Frincke, D. (2000). Concerns about Intrusions into Remotely Accessible Substation Controllers and SCADA Systems. *Twenty-Seventh Annual Western Protective Relay Conference*, *160.* Spokane, WA. Retrieved January 18, 2012, from http://www.selinc.com/literature/literature.aspx?fid=282

Ralston, P. A., Graham, J. H., & Hieb, J. L. (2007). Cyber security risk assessment for SCADA and DCS networks. *ISA Transactions, 46*(4), 583-594.

Raymond, D. R., Marchany, R. C., Brownfield, M. I., & Midkiff, S. F. (2009). Effects of Denial-of-Sleep Attacks on Wireless Sensor Network MAC Protocols. *IEEE Transactions on Vehicular Technology, 58*(1), 367-380.

Stouffer, K., Falco, J., & Ken, K. (2006). *Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems Security, Recommendations of the National Institute of Standards and Technology.* NIST.

Swedberg, C. (2010). UC Davis Winery Tracks Fermentation Via RFID Sensors. *RFID Journal*. Retrieved October 9, 2011, from http://www.rfidjournal.com/article/view/8033

Verton, D. (2003). Blaster Worm Linked to Severity of Blackout. *ComputerWorld*.

Wessel, R. (2007). RFID Keeps Cherries Fresh. *RFID Journal*. Retrieved October 9, 2011, from http://www.rfidjournal.com/article/view/3554

West, A. (2008). Securing DNP3 and Modbus with AGA12-2J. *IEEE Power and Energy Society General Meeting - Conversion and Delivery of Electrical Energy in the 21st Century.* Pittsburgh, PA.

Yu, X., Cecati, C., Dillon, T., & Simoes, M. (2011). The New Frontier of Smart Grids. *IEEE Industrial Electronics Magazine, 5*(3), 49-63.

ZigBee Alliance. (2008). *ZigBee Specification.* Retrieved September 17, 2011, from ZigBee Alliance: http://www.zigbee.org/Specifications/ZigBee/download.aspx

KEY TERMS & DEFINITIONS

Data acquisition framework: The information gathering component of the SCADA system. This consists of the sensors and the communication path to the control center.

Distributed monitoring system: A large scale distribution of sensors deployed to monitor communication over a large number of collection points, feeding that information back to a central computer.

Distributed Network Protocol (DNP3): A set of communication protocols used in industrial SCADA systems.

Human Machine Interface (HMI): A system designed to gather information from the backend and display it in a format that is easily readable by humans.

Industrial Control Systems (ICS): These systems will operate based on information received from remote locations, they can send commands to field devices which control components such as valves and sensors.

Radio Frequency Identification (RFID): RFID stands for Radio Frequency Identification and is a wireless system used to identify objects, which may be people or assets. RFID systems contain RFID readers and RFID tags. Tags are attached to the objects and readers provide the means for the user to interact with the tag.

Remote Terminal Unit (RTU): This unit controls a physical object and communicates that status with the control center. It acts as a means to send digital commands to the physical object.

Machine to Machine (M2M): Machine-to-machine (M2M) communication is defined as any two machines communicating with each other without human interaction. An example of this in a SCADA system includes a sensor communicating with a controller unit.

Microgrid: A small cell of the smart grid, which contains everything needed to run. It has the ability to control and distribute power locally and communicate effectively. By integrating several of these, the Smart Grid will develop.

Programmable Logic Controller (PLC): A computer designed to interact with physical components in order to obtain information about or to control a physical system as well as communicate with other computers.

Supervisory Control and Data Acquisition (SCADA): An industrial control system to monitor a plant or equipment in industry. It entails the control center where decisions are made, remote locations where sensors are placed to gather information, and the communication to connect them.

Situational Awareness: The intelligence and ability to recognize what events are occurring in the system. It includes monitoring, recognizing, and analyzing activity.

Smart Grid: An initiative to upgrade the power grid to modern standards by incorporating current technology and networking to improve communication, situational awareness, and information flow to both customers and providers.

ZigBee: A communication standard designed for low-cost, low-power-consumption wireless communication. Devices generally spend a majority of time asleep, leading to batteries lasting for months or years before requiring a replacement.