

A Situational Awareness Architecture for the Smart Grid

Anastasia Mavridou and Mauricio Papa

Institute for Information Security,
Computer Science Department, University of Tulsa,
800 S. Tucker Dr., Tulsa, OK 74104, USA
{anastasia-mavridou,mauricio-papa}@utulsa.edu

Abstract. Components of the electric power grid that were traditionally deployed in physically isolated networks, are now using IP based, interconnected networks to transmit Supervisory Control and Data Acquisition (SCADA) messages. SCADA protocols were not designed with security in mind. Therefore, in order to enhance security, access control and risk mitigation, operators need detailed and accurate information about the status, integrity, configuration and network topology of SCADA devices. This paper describes a comprehensive system architecture that provides situational awareness (SA) for SCADA devices and their operations in a Smart Grid environment. The proposed SA architecture collects and analyzes industrial traffic and stores relevant information, verifies the integrity and the status of field devices and reports identified anomalies to operators.

Keywords: Cyber Security, Smart Grid, Situational Awareness, SCADA.

1 Introduction

The electric power grid is responsible for reliably and efficiently delivering electricity from generation to the end consumer. Three major components make up the grid: electricity generation sources, transmission system and distribution system. Electric power transmission refers to the bulk transfer of electrical energy, 100 kV and above, from power plants to distribution substations located close to population centers. On the other hand, electric power distribution, which is the final stage of the delivery network, refers to the delivery of electricity from distribution substations to end consumers. Since no energy storage mechanism is used, electric energy requires that system operators control electricity flow, by balancing power generation and consumption, using SCADA systems [1]. Hence, the electric infrastructure is highly dependent on SCADA systems that are responsible for monitoring and controlling all functions in the grid.

The current power grid is based on requirements written in 1950 and it is already considered to be an outmoded, inefficient, vulnerable infrastructure. There have been at least five massive blackouts over the past 40 years that illustrate

problems associated with the power grid [2]. These blackouts have occurred mainly due to faults at power stations, damage to power lines and substations, unusually high demand and others. Also, a cyber attack may have a huge impact on the functionality of the power grid that can result in a blackout. In fact, the massive North East blackout of 2003 has been linked to the propagation of the MSBlaster worm [3] [4].

The need to address these issues, as well as higher demand for quality and availability, penetration of renewable energy resources and the increased threat of terrorist attacks has given birth to the Smart Grid. The Smart Grid is expected to deliver electricity from multiple suppliers to end consumers using two-way communications, involving multiple distributed intelligent entities and including large-scale real-time data collection capability [5]. This large-scale, accurate, and timely data collection and fusion of the monitored processes of the Smart Grid can provide SA. In particular, NIST states that “the goals of situational awareness are to understand and ultimately optimize the management of power-network components, behavior, and performance, as well as to anticipate, prevent, or respond to problems before disruptions can arise” [6]. This paper describes a SA architecture intended to provide Smart Grid operators with a detailed view of the network topology along with information about the configuration, status, critical states and traffic of SCADA devices.

2 Smart Grid Architecture

As technology continues to advance, the power grid is being upgraded with new technologies and additional IT systems and networks. The importance of upgrading the current electricity network is emphasized in President Obama’s speech: “...my administration is making major investments in our information infrastructure: laying broadband lines to every corner of America, building a smart electric grid to deliver energy more efficiently...” [7]. The National Energy Technology Laboratory (NETL) [8] outlined the functionalities of this new electric grid. According to NETL [9], the Smart Grid self-heals, motivates and includes the consumer, resists physical and cyber attacks, increases power quality, accommodates all generation and storage options, enables new products, services and markets, optimizes assets and operates efficiently.

Smart grid modernization is an ongoing process. Smart meters are currently being installed on buildings that enable two-way communication between the utility and end customers. Also, other smart components are added to provide the system operator with SA and the ability to reroute electricity in case of problems in transmission lines. As a result, operators can react and solve system problems in a timely manner to minimize any negative impacts. The main components of a Smart Grid (Figure 1) are electric power generators, electric power substations, transmission and distribution lines, controllers, smart meters, collector nodes, and distribution and transmission control centers [10]. Power generators and electric power substations use electronic controllers to control the generation and the flow of electric power.

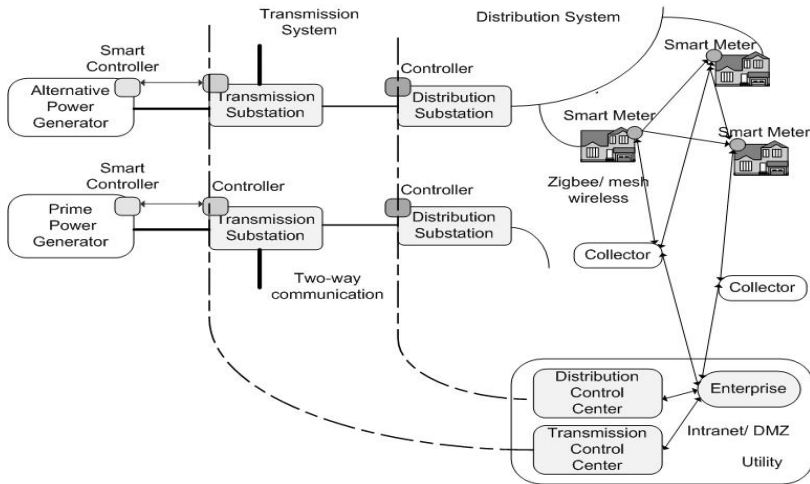


Fig. 1. Block diagram of typical smart grid components and connections

End consumers and collector nodes may communicate through a Zigbee or similar mesh wireless two-way communication network. Two-way communication paths are also used between collectors and the utility. Collector nodes communicate with the utility mostly using the Advanced Metering Infrastructure (AMI) [11] possibly via the Internet. A utility’s intranet includes a Demilitarized Zone (DMZ) to provide extra protection. Additionally, communication between the transmission and distribution substations and the utility’s control center facilitates operation. Like existing power grids, a Smart Grid includes a control system that accommodates intelligent monitoring mechanisms and keeps track of all electric power flowing in a more detailed and flexible way.

3 Security and Reliability Standards and Requirements

The new functionalities provided by the Smart Grid also introduce new security risks due to the transition from legacy (closed) to IP-based (open) networks. In the past, industrial systems were considered to be secure mainly due to the use of proprietary controls and limited connectivity. Smart Grid expands the number and the exposure of SCADA systems, therefore making the protection of these systems a major concern [12].

The National Institute of Standards and Technology (NIST) Cyber Security Coordination Task Group (CSCTG) was established to ensure consistency. NIST, especially after the publication of the NISTIR 7628 document [13], continues to play an important role in shaping Smart Grid Cyber Security research. According to NISTIR 7628, increasing the complexity of the grid through interconnected networks could increase the risk of private data exposure to potential adversaries and unintentional user errors.

The Federal Energy Regulatory Commission (FERC) [14] is responsible for protecting the reliability of the high voltage transmission system. Its mission is to “assist consumers in obtaining reliable, efficient and sustainable energy services at a reasonable cost through appropriate regulatory and market means”. In early 2008, FERC approved mandatory critical infrastructure protection reliability standards designed to protect the nation’s bulk power system against potential disruptions from cyber security threats.

These reliability standards were developed by the North American Electrical Reliability Corporation (NERC) [15], which FERC has designated as the Electric Reliability Organization (ERO). These standards specify the minimum requirements to support the reliability of the electrical system. NERC’s authority is limited to the electrical generation resources and transmission lines. The set of standards addressing cyber-security in the power grid are known as NERC Critical Infrastructure Protection (CIP) standards [16]. NERC requires power transmission companies to be compliant with reliability standards. Table 1 lists and briefly describes the CIP Reliability standards as of June 2011.

Table 1. NERC CIP reliability standards

Number	Title	Description
CIP-001-1a	Sabotage Reporting	Entities are required to maintain procedures for recognizing and making appropriate personnel aware of sabotage attempts.
CIP-002-4	CS-Critical Cyber Asset Identification	Creates risk-based assessment methods for identifying Critical Cyber Assets within a bulk power system facility.
CIP-003-4	CS-Security Management Controls	A cyber security policy ensuring compliance with the other CIP standards must be created and implemented.
CIP-004-4	CS-Personnel and Training	On-going awareness program to reinforce security practices.
CIP-005-4a	CS-Electronic Security Perimeter	Every critical cyber asset must be within an electronic security perimeter (ESP) with documented access points.
CIP-006-4c	CS-Physical Security of Critical Cyber Assets	Requires an annually reviewed security plan approved by a senior manager or delegate for a physical security perimeter (PSP).
CIP-007-4	CS-Systems Security Management	Test procedures must be created to ensure that changes to cyber assets do not adversely affect existing cyber security controls.
CIP-008-4	CS-Incident Reporting and Response Planning	Requires annually reviewed security incident response plans.
CIP-009-4	CS-Recovery Plans for Critical Cyber Assets	Requires the creation and annual review of recovery plans.

Furthermore, SA is recognized as a key enabling functionality for the Smart Grid by FERC [17]. Table 2 summarizes the SA requirements that should be satisfied according to [18].

Table 2. Situational awareness requirements

Requirement	Description
1 Situation perception	Be aware of the current situation. Situation recognition and identification.
2 Impact assessment	Be aware of the impact of the attack. Vulnerability analysis.
3 Situation tracking	Be aware of how situations evolve.
4 Trend and intent analysis	Be aware of actor (adversary) behavior.
5 Causality analysis	Be aware of why and how the current situation is caused.
6 Quality assessment	Be aware of the quality of the collected situation awareness information items.
7 Future assessment	Assess plausible futures of the current situation.

4 Situational Awareness Architecture

The proposed SA architecture provides operators with comprehensive knowledge of the topology and status of SCADA devices and their operations in a Smart Grid, and also allows detection of suspicious incidents. Electric power substations, which are important components of the Smart Grid, contain a number of critical assets such as transformers, circuit breakers, SCADA devices and safety devices. Optimizing the maintenance of these assets is a challenging task. The Critical Infrastructure Lab at the University of Tulsa designed and constructed a scaled-down electric power substation prototype to validate the approach and test functionality.

The design of the substation prototype closely resembles the topology of a ring-type substation with redundant lines. The substation uses power transformers rated at 3KVA and has two three-phase inputs at 240 VAC that are subsequently transformed to 208 VAC. Furthermore, the substation uses Programmable Logic Controllers (PLCs) that communicate over Ethernet using the Distributed Network Protocol (DNP3) protocol [19]. According to Electric Power Research Institute (EPRI) [20], over 75% of North American electric utilities employ DNP3 to control their power systems. DNP3 is an insecure industrial protocol and as a result, security and access control in DNP3 implementations is a major concern.

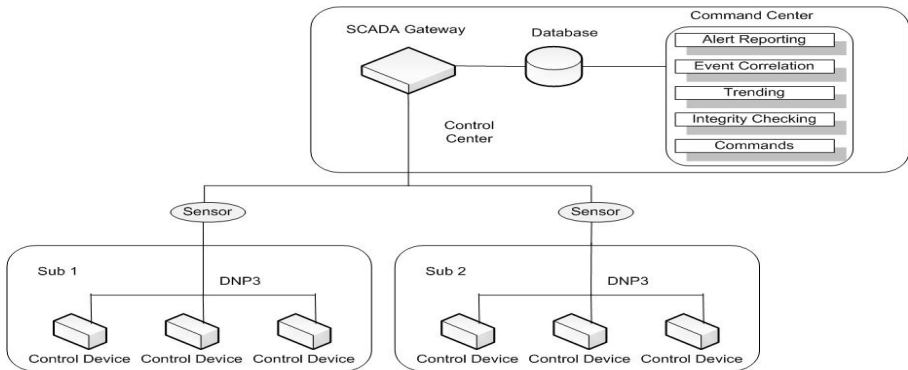


Fig. 2. Situational awareness architecture

The proposed SA architecture (Figure 2) incorporates a SCADA gateway, a database and a command center located in the control center and a number of network sensors placed at strategic points in the field.

Network Sensors. The network sensors operate in promiscuous mode to capture network traffic of interest. As a result, the sensors receive information about network topology, unit configuration, functionality and state of the devices, requested operations, function codes and other important pieces of information.

The sensors timestamp the collected traffic, analyze it and forward relevant information to the SCADA gateway. In addition, they may also help in locating attack signatures to identify malicious traffic. Therefore, simple attacks can be detected where the intent is to interfere with the state of a single field device. Additionally, the sensors receive commands from the command center through the SCADA gateway. Upon receiving a specific command, a sensor may configure its network interface, start and stop scanning activities or generate a traffic analysis report.

SCADA Gateway. The SCADA gateway collects the data gathered by sensors, translates them from different protocols into a canonical format and then forwards them to the database. Communication may also flow in the opposite direction to forward commands concerning configuration settings, scanning and generating reports from the command center to the sensors.

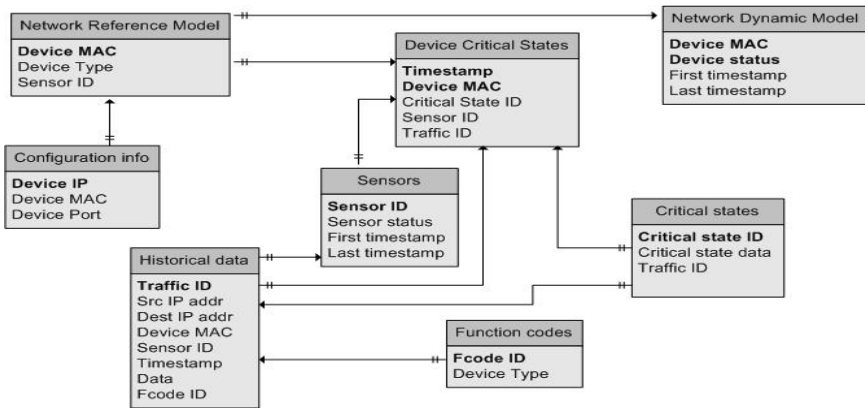


Fig. 3. Database scheme

Database. The database provides a buffering interface between the SCADA gateway and the command center. The traffic stored in the database is used by the command center to provide state based traffic analysis. The database scheme (Figure 3) includes information about system configuration, historical data, the critical states, the network reference model and the network dynamic model. The configuration info contains the configuration settings of the devices such as network addresses, protocols and function codes. Historical information, indicative of inter-task communications data exchange, is stored in the historical data table. In general, network transactions are stored indefinitely for post incident retrieval since they may help in further causality analysis and impact assessment. The network reference model contains, time invariant information such as the network topology. Its counterpart, the dynamic network model includes real time information related to the actual and current status of the field devices.

The critical states table contains the rules that describe all these states, as well as other fault conditions of the system.

Command Center. The command center is a collection of applications that provide facilities for alert reporting, event correlation, integrity checking, trending and command generation. State based traffic analysis is achieved by event correlation and prior knowledge of the critical system states. The command center verifies whether the system may enter into a critical state, as defined by the associated table in the database, and raises an alert. This approach will allow security practitioners to detect complex and coordinated attacks on industrial control systems that may have a negative impact on overall availability and integrity. Time stamps are key elements in supporting the development of an accurate incident timeline from stored transactions. This will help operators in the command center to better recognize adversary intents, capabilities and trends, understand system vulnerabilities and identify new threats.

5 Conclusions and Future Work

A SA architecture designed for SCADA systems in a Smart Grid environment was presented. The proposed architecture combines traditional signature-based techniques and a state analysis technique. More specifically, the architecture aims at satisfying the requirements included in Table 2 in terms of situation recognition (requirements 1 and 6), situation comprehension (requirements 2 and 5) and situation projection (requirements 3, 4 and 7) [18]. Furthermore, Table 3 describes areas in which the proposed SA architecture can help with NERC CIP 001 through 009 compliance efforts.

Table 3. Compliance with the NERC CIP standards

NERC standard	SA architecture
CIP-001-1a	Identifies incidents in real-time monitoring, classifying and alarming on attacks.
CIP-003-4	Provides reporting that helps operation management, security and compliance related decision making.
CIP-004-4	Enhances personnel training by providing situational awareness. Covers areas of awareness that personnel usually cannot.
CIP-005-4a	Monitors the ESP and identifies changes on ESP devices while enhances access control. Alerts upon detecting unauthorized access and correlates detected vulnerabilities with other data to provide cyber vulnerability assessments.
CIP-006-4c	Enhances physical access controls by monitoring the access systems.
CIP-007-4	Monitors and correlates incident data across all devices and enhances Systems Security Management by providing a centralized view of the system.
CIP-008-4	Provides a centralized system for collecting, reporting and responding/alarming on critical events.
CIP-009-4	Provides early warning system failures that may improve response time and diagnostic abilities.

Further research objectives include modeling, simulating and experimentally verifying the behavior of the electric substation control system and providing methods to link the physical and cyber assets of the system. As the architecture is moved from design to implementation, test strategies for validating security and reliability properties of the modeled assets will have to be developed.

References

1. National Communications System: Supervisory Control and Data Acquisition (SCADA) Systems, Technical Information Bulletin NCS TIB 04-1 (2004)
2. U.S. Department of Energy: The Smart Grid: An Introduction (2008), <http://www.oe.energy.gov/1165.htm>
3. Carnegie Mellon University's Computer Emergency Response Team: Advisory CA-2003-20 W32/Blaster Worm (2003)
4. Verton, D.: Blaster Worm Linked to Severity of Blackout, Computerworld (2003)
5. National Energy Technology Laboratory for the U.S. Department of Energy Office of Electricity Delivery and Energy Reliability: The NETL Modern Grid Initiative Powering our 21st-Century Economy: A Compendium of Smart Grid Technologies (2009)
6. National Institute of Standards and Technology: NIST Framework and Roadmap for Smart Grid Interoperability Standards Release 1.0, NIST Special Publication 1108 (2010)
7. President Obama: Remarks by the President on Securing our Nation's Cyber Infrastructure (2009), http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure/
8. National Energy Technology Laboratory, <http://www.netl.doe.gov/about/>
9. National Energy Technology Laboratory for the U.S. Department of Energy Office of Electricity Delivery and Energy Reliability: The NETL Modern Grid Initiative Powering our 21st-Century Economy: Modern Grid Benefits (2007)
10. U.S. Department of Energy Office of Electricity Delivery and Energy Reliability: Study of Security Attributes of Smart Grid Systems – Current Cyber Security Issues (2009)
11. National Energy Technology Laboratory for the U.S. Department of Energy Office of Electricity Delivery and Energy Reliability: Advanced Metering Infrastructure (2008)
12. Electric Power Research Institute: Report to NIST on Smart Grid Interoperability Standards Roadmap, Contract No. SB1341-09-CN-0031-Deliverable 7 (2009)
13. National Institute of Standards and Technology: Guidelines for Smart Grid Cyber Security, Vol.1, Smart Grid Cyber Security Strategy, Architecture, and High-Level Requirements, NISTIR 7628 (2010)
14. Federal Energy Regulatory Commission, <http://www.ferc.gov/about/ferc-does.asp>
15. North American Electric Reliability Corporation, <http://www.nerc.com>
16. North American Electric Reliability Corporation: Reliability Standards for the Bulk Electric Systems of North America (2010), http://www.nerc.com/files/Reliability_Standards_Complete_Set.pdf
17. Federal Energy Regulatory Commission: Smart Grid Policy (2009)
18. Barford, P., Dacier, M., Dietterich, T.G., Fredrikson, M., Giffin, J., Jajodia, S., Jha, S., Li, J., Liu, P., Ning, P., Ou, X., Song, D., Strater, L., Swarup, V., Tadda, G., Wang, C., Yen, J.: Cyber SA: Situational Awareness for Cyber Defense. In: Jajodia, S., Liu, P., Swarup, V., Wang, C. (eds.) Cyber Situational Awareness, pp. 3–13. Springer (2010)
19. Curtis, K.: A DNP3 Protocol Primer, Technical report. DNP Users Group (2005), www.dnp.org/About/DNP3%20Primer%20Rev%20A.pdf
20. Electric Power Research Institute: DNP Security Development, Evaluation and Testing Project Opportunity (2008)