Power Infrastructure Security: Fundamental Insights of Potential Cyber Attacks and Their Impacts on the Power Grid†

Dong Wei [1], Yan Lu [1], Paul Skare [2], Mohsen Jafari [3], Kenneth Rohde [4], and Michael Muller [3]

[1]Siemens Corporate Research, Inc., Princeton, NJ 08540 USA
[2]Siemens Energy Inc., Minnetonka, MN 55305 USA
[3]Rutgers University, New Brunswick, NJ 08855 USA
[4]The Idaho National Lab, Idaho Fall, ID 83415 USA

***Abstract*-- The information infrastructure for the power networks was often viewed as a collection of individual communication channels, separate databases, multiple systems, and different protocols. Automation systems and controller nodes performed minimal monitoring on data and information availability, validity, and integrity. Like any other industry sector, the electrical power industry is facing challenges involved with the increasing demand for interconnected system operations and control under the restructured electrical industry due to deregulation of the electrical market. This moves automation networks from outdated, proprietary, closed networks to the more current arena of Information Technology (IT). However, while gaining all of the cost and performance benefits of IT, existing IT security challenges are acquired as well. The power T&D automation network has inherent security risks due to the fact that the systems and applications in the network were not originally designed for the general IT environment. In this paper, we propose a conceptual layered framework for protecting power T&D (transmission and distribution) automation systems against cyber attacks. The following factors are taken into account: 1) integration with existing, legacy systems in a non-intrusive fashion; 2) desirable performance in terms of modularity, scalability, extendibility, and manageability; 3) alignment to the "Roadmap to Secure Control Systems in the Energy Sector" [1] and the future intelligent power delivery systems [2-4].**

***Index Terms* — power grid, cyber attacks, network security, vulnerability, power grid automation system, QoS (Quality-of-Service)**

I. Introduction

The recent discovery that hackers have inserted software into the US electrical grid [5], which would allow the grid to be disrupted at a later date from a remote location, clearly demonstrates the fact that the utility infrastructure is quite vulnerable and that its overall mission of serving the population could be severely compromised as a result of unexpected man-made or natural disasters.

As other industry sectors are already experienced with arming automation systems with modern IT technology, electrical power industry is also facing the trend of integrating the electrical infrastructure with information infrastructure, which is so-called "Smart Grid" [2-4]. This integration not only moves power automation systems from outdated, proprietary technology to the use of common technologies – personal computers, Microsoft Windows and TCP/IP/Ethernet, but also brings the closed network of power control system to the public network. The integration brings in tremendous cost and performance benefit to the power industry, as well as arduous challenges of protecting the automation systems from security threats from hackers. It is misleading to suggest that IT people take the full responsibility for power grid network security including automation and control networks. Compared with regular IT systems, power automation systems have definite different goals, objectives and assumptions concerning what needs to be protected. It is important to understand what "real time performance" and "continuous operation" of a power automation system really means and to recognize that power grid automation systems and applications were not originally designed for the general IT environment. Therefore, it is necessary to embrace and use existing IT security solutions where they fit, such as communication within a control center, and develop unique solutions to fill the gaps where IT solutions do not work or apply.

This article, from an automation engineer's point of view, presents an in-depth analysis on the current power automation system's configurations, communication specifications and associated vulnerabilities, as well as the potential cyber attack sources, scenarios and the adverse impacts on power network. The authors have conducted intensive study on all of the important aspects of potential cyber attacks on the power grid and tried to provide a comprehensive survey for power automation system designers and control system security researchers to use. Armed with this information, we will have a greater chance of successfully securing the critical power infrastructure.

II. Potential Cyber Attacks and their Adverse Impacts on Power Automation System

Today, in order to deliver electrical power from power producers to consumers economically, the power T&D system operators have to exchange data with power producers, ISO/RTOs, consumers, and peer system operators

† This work is part of the project "Protecting Intelligent Distributed Power Grids against Cyber Attacks", which was conducted for the DoE Office of Electricity Delivery and Energy Reliability under Contract DE-FC26-07NT43313.

at two different levels – corporate and control/operation center. The power T&D system operator also possesses communication links between corporate and control centers, and control centers and substations. The expansion of today's power T&D communications network incorporates multiple topologies, several types of communication protocols, and varying QoS requirements throughout the system.

The complicated information communication network makes power T&D automation systems in a more vulnerable position to cyber attacks. The Vulnerabilities in Power T&D Automation Systems exist at all levels of the control system, including *Component, Protocol*, and *Network.* With identified system vulnerability, the cyber attackers become more and more skilled at launching cyber attacks to power grid. The typical attack process can be broken down to the three necessary steps: *access*, *discovery*, and *control*. The first step of a cyber attack is to gain access to the SCADA system through either corporate to SCADA network communications or external Virtual Private Network (VPN) access and remote site communications. Once access is obtained, the attacker must discover the SCADA process, attempting to understand the system mechanisms in order to successfully launch an intelligent attack. After the SCADA process is understood by the attacker, he will attempt to control *FEP, Application Server, HMI, EWS*. Database System and even directly the controllers.

The whole purpose of a cyber attack is to cause some sort of adverse impact on whatever the perpetrator is targeting. Two specific types of impacts are primarily concerned with the power T&D automation system: *safety* and *operational*. Impacts regarding safety refer to a degrading of human health or even a loss of life. Operational impacts, on the other hand, can be classified into three levels. The first one is a blackout, which is the worst case operational scenario. The second impact is a brownout, in which the power quality is degraded, with effects such as low voltage or low frequency. The third possible impact involves shifting the power T&D system from its optimal point of operation, resulting in an economic loss for the system operator. All three of these operational impacts will ultimately disrupt any services using electricity, thus affecting anyone located in the targeted areas.

III. Why the existing IT security solution cannot be employed directly?

The comprehensive analysis of potential cyber attacks and their adverse impacts on power T&D automation system reveals that the security requirements of power grid automation system can be classified into four specific categories: integrity, confidentiality, availability, and non-repudiation, which is different for the regular IT security requirements focusing only on connectivity.

Hence, even though the IT industry has witnessed the development of many effective cyber security solutions to protect corporate and other IT networks--from firewalls to intrusion detection systems and VPNs, we may not directly deploy existing IT security solutions in power T&D automation systems due to the major differences between IT and control network. To summarize, they have different security objectives, different security architecture different technology base, and different performance requirements. These major differences between IT and control networks lead to gaps between IT-based security solutions and power T&D automation system security requirements. These differences also indicate that a new systematic approach should be developed to meet the requirements of power T&D automation systems. However, some of the existing IT security techniques can be transplanted into power T&D automation networks. Some security requirements for automation networks are actually less demanding than those for corporate networks.

IV. Major Challenges to secure power grid

- The current power infrastructure was designed for performance rather than security. Most automation components (RTU, PLC, etc.) use proprietary operating systems, which were designed for control functionality and performance, but not security. Likewise, communications protocols employed were designed for bandwidth efficiency without the consideration of cyber security.
- The future state of the power grid is uncertain, though the trend seems to be a steady movement towards a smart grid. One thing is for sure – the power grid is undergoing sustained growth in order to keep up with the mounting demand for electricity.
- Security and automation have existed in two separate domains and as a result, evolve at different paces. Automation systems are usually a combination of new and legacy components, the latter of which may not have enough reserved resource to perform security functionalities.
- Network security solutions have been tailored for the IT world, without regarding performance requirements for automation systems.

V. Guidelines to secure power grid against cyber attacks

- The new security solutions must be scalable in order to maintain the same level of growth experienced by the power grid. The security performance of the solution must remain undiminished as the power infrastructure size increases.
- The new security solutions must be extensible, *i.e.*, be able to handle any future state of the power grid, including new technologies and communication protocols. Measures should be taken to avoid early obsolescence when the solutions are developed.

- It should be possible to integrate the new security solutions into the existing, legacy systems in a non-intrusive fashion without compromising their control performance, reliability, stability, and availability. The solution should be able to achieve a balance between security and automation system performance.
- New solutions should support standard security services and be able to integrate security management (such as authorization and authentication), security operations (such as logging and auditing), and other security technologies (such as access control and intrusion detection).

VI. Strategy

To meet the challenges of protecting the power T&D automation systems against cyber attacks, we propose an *integrated security framework,* also called *common security platform,* as shown in Fig. 1. In The automation and control system monitors and controls power transmission and distribution processes, while the security layer provides security features. Since the security layer provides clear demarcation of responsibilities, control functionalities and security functionalities can be decoupled. Data related to security management flows on this layer.

Our idea is that this platform could be used by various power T&D automation system vendors/users who can build their security products on top of it. Therefore, the new security system should be extensible and customizable for future intelligent power grid automation systems. It should be possible to integrate the new security system into the existing, legacy systems in a non-intrusive fashion without compromising their control performance, reliability, stability or availability. Our platform will support security management (such as authorization and authentication), security operations (such as logging and auditing) and access control and intrusion detection technologies in an integrated fashion.

While designing and operating the security system, it can mitigate vulnerabilities and maximize security performance with given data from both the power layer and the A&C layer (such as power flow, hardware configuration, network configuration, QoS data). The proposed framework integrates security management (such as patch, personal access control policy), security operation (such as user access and user activity logs) and security technology (such as firewall, intrusion detection).

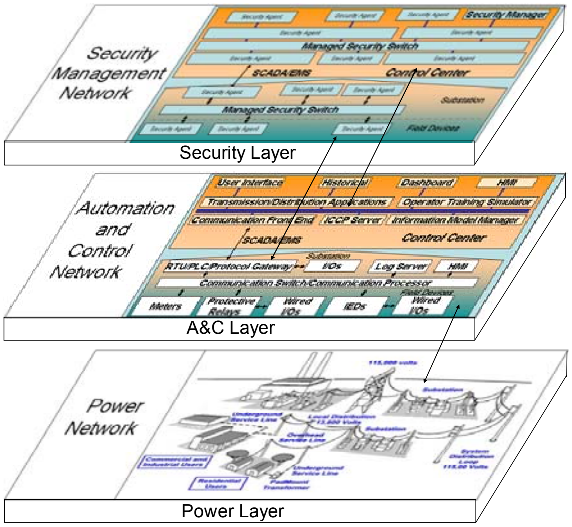

Figure 1: The 3-layered power transmission and distribution system

VII. Acknowledgment

The authors would like to express their gratitude to Dr. Diane Hooie of the Department of Energy who provides overall project management, with support from the DoE contract manager Jeffrey Kooser and Tom Flowers. The authors gratefully acknowledge the contributions of Salman Siddiqui, Chao Zhang, Kun Ji, Hongming Jin, and Prithvi Raju for their work on the prototyping development.

References:

[1] U.S. DOE & Department of Homeland Security, Roadmap to secure control systems in the energy sector, January 2006.

[2] "The Smart Grid: An Introduction", a DoE report prepared by Litos Strategic Communication.

[3] Massoud Amin, S.; Wollenberg, B.F., "Toward a smart grid: power delivery for the 21st century," *Power and Energy Magazine, IEEE*, vol.3, no.5, pp. 34-41, Sept.-Oct. 2005

[4] Gellings, C.W.; Samotyj, M.; Howe, B., "The future's smart delivery system [electric power supply]," *Power and Energy Magazine, IEEE*, vol.2, no.5, pp. 40-48, Sept.-Oct. 2004

[5] Siobhan Gorman, "Electricity Grid in U.S. Penetrated By Spies", *The Wall Street Journal*, Page A1, April 8, 2009.