Smart Grid Cybersecurity

Exceeding cybersecurity requirements mandated by customers and regulatory agencies

Abstract

The world has become much more connected, with over 32 percent of the population of the planet, or 2.3 billion people, having access to the Internet. Like individuals, systems that control electric power generation and distribution are becoming more connected. Traditionally, these systems have been:

- Few in number
- Localized to a comparatively few locations (such as control rooms, generating plants and substations)
- Isolated from public networks, making them relatively easy to secure.

It was often possible to provide a high degree of security through simple physical measures like fences and locks on doors. Smart Grid technology changes this by placing large numbers of intelligent devices into places where they are often easily physically accessible and by placing many of them onto networks that may be physically accessible, or indirectly logically accessible from public networks.

Touch points between utility networks and public (or nearly public) networks will become more numerous and widespread. Systems that could once be contained within a locked “six-wall” room will become widely distributed, with inexpensive networked devices on individual houses and apartments.

The rapid evolution of the Smart Grid promises to pose new cybersecurity challenges for at least the next several years.

Point of View (POV) Executive White Paper Series

These executive white papers provide valuable insight into the innovative application of technology to solve business problems that are confronting utilities, municipalities and other Smart Grid related organizations. The papers should serve as a helpful resource to aid chief financial officers (CFOs) and chief executive officers (CEOs) in discussions with institutional chief information officers (CIOs) in the exploration of new methods and processes for reducing costs.
Executive summary

Industrial control systems (ICS), particularly those used by electric and other utility companies, formerly had few, if any, connections to the world outside the corporation that owned and operated them.

In response to trends like deregulation and the growth of alternative and widely distributed energy sources, data collected and used by control systems has increasingly been both obtained and exchanged via public networks. Interconnections between neighbor and partner utilities and independent system operators have also increasingly made use of public networks.

Control centers and substations have traditionally been critical, physical assets. They have now become part of an increasing inventory of cyber assets which can no longer be secured simply by placing them behind fences and locked doors.

Open standards are replacing proprietary hardware/software
True security requires more than simple compliance with applicable standards and will require a number of actions to assist users in achieving both compliance and security.

Cybersecurity for the Smart Grid is in flux. We know how to secure traditional systems like a supervisory control and data acquisition systems (SCADA), energy management systems (EMS) or distribution management systems (DMS). For these systems, familiar techniques like firewalls, role-based access controls, multi-factor authentication, and anti-malware measures can still be used to provide a high degree of security.

There has been a dramatic evolution from using proprietary hardware and software toward using off-the-shelf hardware and software. There has also been an equally dramatic evolution from traditional, proprietary communications protocols toward standards-based approaches, notably DNP3 or IEC 61850 for grid control. While a cybersecurity professional will say that "security through obscurity" is never an appropriate defense, the reality is that the move to standard hardware and software has enabled the greater connectivity we see today. In turn, that increased connectivity can make an attacker’s job easier.

Effective cybersecurity must protect critical assets
The world has simply become a more dangerous place for computers and networks. Today, networks are under assault from a wide variety of rogue governments and pseudo-governments, terrorists, criminals and people who see breaking into computer systems as a challenging game.

The rise of the Internet and the Web have revolutionized how the world communicates, conducts business, entertains itself and participates in countless other activities no one could have even imagined a few decades ago. Internet technologies have also revolutionized the electric utility industry. Developments include:

- Substation equipment can now be configured from hundreds of miles away over a network.
- A SCADA one-line diagram can be viewed with a Web browser on a laptop in a substation or in a service truck.
- Information can quickly and efficiently be exchanged between companies, asset owners and partner utilities.
All of these are good things – they allow electric utilities to utilize resources more efficiently, maintain them more effectively, increase business agility and be more responsive to customer needs.

**With improved technology comes new criminal behavior**
As keepers of much of the world’s critical infrastructure, it is the job of the electric utility to do everything within reason to prevent malicious or accidental damage to critical resources that are in their care. Recent initiatives for international cybersecurity standards, promoted by the White House, the United States Department of Homeland Security (DHS) and governments around the world make this document relevant to the worldwide energy industry.

Power utilities are an important national cybersecurity concern because of the essential nature of electricity in our life. Control centers, generators and other facilities have always been critical to the delivery of electric power, and the number and the variety of these critical assets continues to increase.

**Security challenges**

**What is the potential for critical infrastructure attacks or a major breach of our electrical power grid?**
In the cybersecurity community, despite frequently heard statements such as “a well-funded, highly motivated, intelligent adversary can eventually defeat any cybersecurity,” successful attacks against critical infrastructure have been rare.

Nevertheless, security professionals would most likely say that the “attack surface” of systems is dramatically increasing.

**Smart Grid benefits bring new cybersecurity challenges**
Smart Grid technologies and devices promise great benefits in a number of areas: reduced cost, increased reliability and even reduced environmental impact. As a result, there has been a rush to design, develop and deploy these technologies and devices. In this rush, cybersecurity has not always received the attention it deserves.

**How SCADA security is different from smart metering security**
In large part, the difference between SCADA security and smart metering security can be expressed simply as concentrated vs. distributed. A SCADA system is generally in one room (albeit with links to devices in substations, which are themselves for the most part in one room). Smart metering is everywhere – and it is not possible to build a fence with a gate and a lock around “everywhere.”

**Is cybersecurity a good investment?**
Corporate management brings a special set of concerns toward cybersecurity. When managers are considering adding or upgrading facilities or equipment, return on investment (ROI) is a major factor in their deliberations. ROI is also a strong concern for shareholders.

With cybersecurity, ROI is somewhat nebulous. While it is clear that Smart Grid technologies offer increased value, reliability and sustainability, one of the challenges for the future is how to quantify cybersecurity investments in an industry where no news is good news (in terms of cybersecurity threats). As a result, finding a clear and quantifiable answer to this question will continue to remain a challenge.
Cybersecurity challenges for utility operators

There are a number of factors that make cybersecurity a complex challenge for utility operators:

- Modern SCADA/EMS/DMS systems are large, complex and incorporate increasingly large numbers of widely distributed components.
- The distributed nature of SCADA/EMS/DMS systems results in complex network architectures.
- SCADA/EMS/DMS systems and networks employ a wide variety of cybersecurity equipment and software.
- Utilities require processes to manage, monitor and maintain these assets which can be complex and resource intensive.
- Those who seek to harm energy delivery infrastructures continue to grow in sophistication, number and level of dedication.

Often, especially for small to medium-sized electric utilities, SCADA/EMS/DMS operators do not have 24/7 on-site support from an IT department. It is unrealistic (and potentially dangerous) to expect that grid operators possess sufficient expertise in security related topics to recognize, analyze and deal with the variety of cybersecurity incidents that can occur in today’s world.

Emerging Smart Grid cybersecurity technologies

Securing large, widely dispersed and easily accessible networks pose some significant challenges. For example, in a more traditional setting, support personnel are near at hand to deal with an intrusion. However, if an intrusion occurs in an inexpensive smart meter 100 miles from the nearest support technician, we are faced with an entirely new cost vs. benefit calculus:

- Should a service truck be sent immediately or is it better to wait?
- How long is too long to wait?
- How long might it be before an intrusion into one meter is used by an attacker to attack neighboring meters or other equipment?

“Defense in depth” has long been a popular approach to securing cyber assets whereby a series of obstacles are constructed that an attacker must defeat to breach the core of a system. Defenses have traditionally been in the form of firewalls, intrusion detection systems and malware detection software. To provide defense in depth for the Smart Grid, the same types of techniques can be used, but they need to be more compact, much less expensive, more autonomous, more distributed and require less human attention.

Smart meter security demands creative solutions

Some amazingly creative security solutions are beginning to emerge in the Smart Grid arena. One promising example is a hardware-based intrusion detection system that could be incorporated into a single, integrated circuit that is estimated to cost less than one dollar – that’s cheap enough to allow one to be put into every single smart meter. The solutions are out there and new ones are emerging. The industry just needs to allow and encourage creative people to find them.

Smart Grid security needs to become part of the corporate culture

A major key to getting serious about security is to move from an environment where the primary concern is compliance to one where the primary concern is security. The difference between compliance and security is sometimes subtle, but it can have a large impact. For example, current NERC CIP rules mandate that anti-malware software be installed and maintained on critical cyber assets. If you follow those rules, you are compliant. However, since current anti-malware solutions are notoriously ineffective at dealing with zero-day threats, compliance does not equal security in this case. A corporate culture that is concerned not only with compliance but also security will encourage better solutions.
Case Study – Cybersecurity Manager (CSM)

Cybersecurity Manager is designed to help shift the odds in the “good guys” favor
As part of an effort to help improve the cybersecurity posture of the energy delivery infrastructure of the United States, the U.S. Department of Energy (DOE) has funded development of CSM by Siemens and the Pacific Northwest National Laboratory.

CSM is not intended to replace existing tools used by IT staff. However, it is designed to provide a tool that will help an EMS operator recognize and respond to cybersecurity incidents without requiring the operator to be an expert in cybersecurity, networking, or the tools that a security professional would typically use.

Unique to CSM is its integration into an existing operator training simulator (OTS):

- Operators can be trained to use the tool by working through realistic simulations or a replay of real-life situations.
- OTS allows an administrator to use a simulation to test CSM configuration changes.

Development and demonstration of a security core component
The SCADA and EMS systems used by the electric utility industry to monitor and control electric power generation, transmission and distribution are recognized today as critical components of the electric power delivery infrastructure. SCADA/EMS operators are traditionally very accomplished at managing the power grid, but are frequently not trained to manage cybersecurity aspects of today’s complex equipment and networks.

CSM will assist operators and provide new OTS tools that will facilitate training and practice to recognize and handle cybersecurity incidents.

The Siemens cybersecurity advantage

Siemens’ Smart Grid cybersecurity team supports our customers and Siemens’ internal business units. The team develops and implements tools and methodologies required to provide a secure, reliable computing and network infrastructure. Our approach emphasizes:

- Soliciting and understanding customer requirements and responding effectively to customer requests and concerns.
- Emphasizing a proactive approach, where we not only maintain a high awareness of relevant regulations and standards, but actively participate in influencing the development of those standards.
- Actively developing and maintaining Siemens’ internal processes so that cybersecurity is the responsibility of all Siemens employees, at all levels of the organization and throughout the entire product lifecycle.
- Developing and offering cybersecurity related products and services that are reliable and secure, enhancing our customers’ ability to deploy and use these products to improve the reliability and security of the energy delivery system (Illustrated in figure 1 on the next page).

CSM is designed to provide a tool that will help an EMS operator recognize and respond to cybersecurity incidents without requiring the operator to be an expert in cybersecurity.

CSM assists operators, who are frequently not trained to manage cybersecurity aspects of today’s complex equipment and networks.

Siemens’ proactive approach enhances customers’ ability to improve the reliability and security of the energy delivery system.
Helping customers achieve compliance

Compliance and security are related but not equal. Siemens thinks of compliance as a subset of the larger topic of cybersecurity. Effective security requires more than simple compliance with applicable standards – in Siemens’ case, we have implemented a number of actions to assist our customers in achieving both compliance and security.

As a worldwide vendor, Siemens delivers systems to customers that are governed by a host of different security regulations. One common thread through all these regulations includes maintaining a secure energy delivery infrastructure that requires a partnership between system owners and the vendors who supply those systems.

Our goal is to help our customers achieve compliance with relevant security regulations, and to help ensure that Siemens has done everything feasible (from both product and process points of view) to make sure our customers’ systems are both compliant and secure. Our approach is described below.

A proactive cybersecurity approach
Siemens is an acknowledged world leader in supplying products and services to the electric utility industry, with extensive experience in cybersecurity. We have been called twice to testify before the U.S. Congress on the topic of security in the electric utility industry. We closely follow numerous security-related standards, including the North American Electric Reliability Corporation critical infrastructure protection (NERC CIP) 002-009, Common Criteria, International Organization for Standardization (ISO) 17799 as well as emerging standards.

We offer the benefit of our technology and experience to help electric utilities achieve the level of cybersecurity that the challenges of today’s world demand. We have developed a suite of security-related products and services that are directed both at owners of Siemens Spectrum Power™ control center products and owners of non-Siemens products.
Cybersecurity standards
As a supplier of a broad range of products, systems and solutions to power transmission and distribution organizations around the world, we keep a close watch on existing and emerging standards worldwide. These include:

- NERC CIP standards in North America
- ISO/International Electrotechnical Commission (IEC) 15408 (Common Criteria)
- ISO/IEC 27002:2005 (formerly ISO/IEC 17799)
- Various National Institute of Standards and Technology (NIST) and other security-related standards and recommendations

Siemens Computer Emergency Readiness Team (S-CERT) employees are active in these organizations, providing industry practical insight and market feedback on the application of existing and emerging standards.

Siemens CERT
S-CERT provides an independent and trustworthy partner for organizations throughout Siemens to deal with cyber-security related issues. S-CERT members hold a variety of cybersecurity and other applicable industry certifications.

S-CERT provides a variety of services, including:

- A central monitoring and notification service for security vulnerability announcements, applicable third-party tools and products used throughout Siemens. This service is integral to Siemens in its overall approach to timely announcements to our customers regarding the availability of security patches that apply to our systems.
- Performing thorough security assessments of Siemens products; future releases of Spectrum Power will be assessed by S-CERT.
- Cyber vulnerability assessments (CVA) on customer systems.

S-CERT’s experience and expertise is an invaluable tool when responding to cybersecurity incidents and customer concerns.

Software subscription agreement (SSA)
The software subscription agreement (SSA) service enables customers to take advantage of Siemens’ continuing investment in the development of the base Spectrum Power system. Every year Siemens invests a significant amount in research and development to enhance and extend the capabilities of Spectrum Power.

Our global development organization is continuously improving the Spectrum Power product line, with the intention of ensuring that system components, including third-party components, are up-to-date for security patches and updates.

System improvements from R&D are generally made available on a regular basis through base system software releases.

Authors
Mayur Rao
Head of Cybersecurity
Siemens Smart Grid Division

Dave Taylor
Certified Information Systems Security Professional (CISSP)
Siemens Smart Grid Division

Andy Turke
Certified Information Systems Security Professional (CISSP)
Siemens Smart Grid Division
Conclusion

Effective cybersecurity requires the latest and best technology and know-how in a fast-moving electric utility field. It also requires a reliable partner that:

- Has industry experience
- Understands the problems electric utilities face
- Has made the commitment to stay abreast of the latest developments in the field
- Has a commitment to train its workforce.

As a leading supplier to electric utilities, Siemens has developed a cohesive cybersecurity response program.

The ongoing convergence of a number of trends over the past several years has led to a continuous elevation of the importance of cybersecurity in the systems that Siemens designs, develops, delivers and supports. These trends have led to a greatly heightened awareness of cybersecurity among media, politicians, standards organizations, government agencies and utilities.

Because of the essential nature of electricity to our economy and lives, power utilities are an important national cybersecurity asset. Through all the details of this process, Siemens is committed to helping customers not only achieve compliance, but move toward a truly effective Smart Grid cybersecurity system.

Siemens Smart Grid Division cybersecurity team

Siemens’ Smart Grid cybersecurity team specializes in designing and building control center and substation products, systems and solutions with a strong emphasis on security. Core attributes of the team include:

- Team members hold Certified Information Systems Security Professional (CISSP) certifications, participate in security conferences and have attended third-party security training.
- The average security team member has more than 20 years of experience in the industry.
- The team is involved during all aspects of Siemens’ standard product development and deployment life cycle, including post-deployment customer support.

Additionally, Siemens offers customers access to this valuable knowledge base through a broad range of consulting services.

Siemens Smart Grid Division

The Siemens Smart Grid Division supplies products and solutions for intelligent and flexible electrical network infrastructures. To meet growing energy needs, the networks of today and tomorrow must integrate all forms of power generation and ensure bi-directional energy and communication flows. Intelligent networks help make it possible to generate and use power efficiently and on demand. They contribute to the electrification of railroads and also supply industrial enterprises, infrastructure elements and entire cities with electricity. For more information, visit www.usa.siemens.com/smartgrid.

For more information about the Siemens Smart Grid division on our on our mobile website, please scan the QR code below.