Making sense out of Smart Grid cyber security standards

Introduction
With all the groups and committees working on the Smart Grid’s security requirements, one might expect that there would now be a recipe for making an automation system secure. But we’re finding that building secure automation systems is more complex than we anticipated.

Most of us have some degree of familiarity with information security as it is practiced in our corporate environments. We may find it annoying at times, but we trust our Information Technologies (IT) people to protect the confidentiality and integrity of the data residing in business systems. This includes our mail servers, file servers, and financial systems. To keep them secure, our IT staff uses a variety of tools, including standards, best practices, and automated security technologies.

On the other hand, a utility that initiates a Smart Grid project generally will be deploying thousands, or even tens of thousands, of relatively inexpensive devices with limited computing capabilities. These devices are deployed for the long term, and may require an expensive truck roll to update a firmware version or to change a setting. The group managing the automation system not only is tasked with ensuring the confidentiality and integrity of data, but also system availability. The system cannot be shut down for maintenance because it’s needed to keep the lights on.

Adding security to an RFP
After recognizing the need for a secure Smart Grid, the U.S. Department of Energy (DOE) required that utilities receiving federal funding had to develop a cyber security program. Challenged with this new requirement, utilities turned to consultants or simply requested security from their vendors. Suddenly, a new “Security” section started appearing in RFPs with an exhaustive list of security standards, giving the impression they were copied from Wikipedia® online encyclopedia.

Vendor solutions now have to comply with NERC CIP-002 to CIP-009, NIST 800-53, NIST 800-82, NIST IR 7628, ISO 17799/27002, and the Department of Homeland Security (DHS) “Catalog of Control Systems Security,” to name just a few. But, anyone familiar with security standards could point out that many of these do not apply to product vendors, but rather define security requirements that the organization itself must meet.
Making sense out of new standards

Power industry professionals are familiar with the NERC CIP standards. These define auditable security requirements for utilities. While they provide valuable security guidance, they are not directly relevant to Smart Grid applications, and primarily target the automation systems used in generation and transmission facilities.

Another major set of guidelines is the “NIST IR 7628 Guidelines for Smart Grid Cyber Security.” These provide a comprehensive set of high-level security requirements for all aspects of the Smart Grid. However, a utility engineering working on a Smart Grid project will probably be overwhelmed by this three volume, 600-page encyclopedic document. In addition, the document provides high-level guidance, not directly actionable engineering specifications.

In the author’s opinion, the Advanced Security Acceleration Project for the Smart Grid (ASAP-SG) provides the most accessible security guidance for Smart Grid projects. This utility-driven, public-private collaborative project has developed security profiles for Advanced Metering Infrastructure (AMI), Distribution Management (DM), and Wide-Area Monitoring Protection and Control (WAMPAC). The group is also working on a Substation Automation (SA) profile.

For instance, the ASAP-SG security profile for Distribution Management addresses the security requirements of Smart Grid applications such as Fault Location, Isolation, Service Restoration, Voltage Optimization and Control, VAR Management, and Integrated Volt/VAR Control.

Further, the ASAP-SG security profiles use an engineering approach that starts by analyzing the applications and their use cases, defines the possible failure modes, and then recommends security controls referenced from the DHS “Catalog of Controls System Security” to prevent these failures.

Let’s outline these security controls and examine how they can help us build a more secure Smart Grid system.

Policy controls

Policy security controls are the foundation of every security standard and framework. Security policies are used to define requirements for training and electronic and physical access control. They also are used for regular security assessments, incident handling and disaster recovery procedures, and configuration management.

For the Smart Grid automation engineer, policy controls are the least exciting and the most difficult to implement. However, they are necessary as technical security controls will only work if they can be enforced. Executive-level support will be needed as effective security demands commitment, efforts, and resources.

Network segmentation

The first technical requirement is to design the network architecture so that it isolates field devices and applications from the external world. While we have become used to relying on the Internet to exchange information, the system should not be built on a public network. Even if a Virtual Private Network (VPN) is used, public networks provide no control, ownership, or guarantee of service. The Smart Grid application should use alternative solutions such as wireless communications or cellular networks in a private mode.

Then, the communications network should be divided into independent segments with well-defined communication paths. The field devices will only communicate with the control application, which will reside in its own network segment. The control application will only communicate with field devices and user workstations that are located in a separate segment, isolated from the business network. The only segment that will have access to the Internet is the business network.

Using this segmented architecture reduces the risk of an external threat compromising the application or field devices. However, it will also make maintenance more difficult by prohibiting external vendor access.

At this step of the system design, we can benefit from the expertise of existing utility IT staff. Securing the control application of a distribution automation system is similar to securing any other enterprise system. However, as we move out into the field, the situation changes and new, less familiar technologies are introduced.
Technical security controls

Whenever people with IT backgrounds spell out technical security requirements, they often request security controls and features that are nonexistent in typical field devices. Centralized authentication, granular access permissions, access logs, and secure communications are generally only available on Windows® or Linux™ machines. Most field devices don’t even have login accounts; only password-protected levels.

While the ASAP-SG security profiles do specify some of these security controls, they also require additional controls that are better adapted to the reality of the Smart Grid.

Protecting a field device

To illustrate the ASAP-SG security profile approach, let’s consider a field device such as a recloser or a capacitor bank controller. The device typically will be deployed in a cabinet, and will be connected through wireless or cellular communications. A malicious individual breaking into a cabinet could disrupt the operation of the application by disabling the device, feeding it false information or gaining access to the control system through the communications link.

The security profile uses a systems engineering approach. The first step is to lock the cabinet to protect the device. Ideally, the locking mechanism should grant users permission on a per-cabinet basis and require periodic re-authorization to protect against lost keys and disgruntled employees.

Because it is next to impossible to completely protect the cabinet, the system shall provide means to monitor that the device is operating correctly, detect any breach or failure, and report it to the control application. The control application should be able to isolate a compromised or defective field device.

The security profile defines additional controls to further improve the security, and thus the reliability of the system. Access monitoring should continue to operate in the event of a power failure. The state of the power source should be monitored and logged as an unexpected power loss could indicate a breach. The device should monitor and report its health, and validate its firmware and settings.

Securing communications

Once physical integrity of the device is ensured, we need to protect communications with the application. Part of the solution is to use encryption to ensure data confidentiality and to provide a certain level of authentication. While encryption is often considered the “cure-all” security solution, deploying it on a large scale is complex. Further, the encryption algorithms and protocols should comply with approved standards, or the utility will be tied to a specific vendor and even risk data exposure.

The “NIST Framework and Roadmap for Smart Grid Interoperability Standards” recommends the IEC 62351 standards for secure SCADA communications. These standards provide guidelines on the use of the Transport Layer Security (TLS) protocol for data encryption. The standards also define a challenge-response security mechanism to ensure the security of control operations. This mechanism has been implemented in the DNP3 protocol as the Secure Authentication function.

Both encryption and secure authentication will require an automated key management mechanism, which brings us back to the enterprise level.

Managing devices

As previously mentioned, we need to manage keys if we use cryptography or DNP3 Secure Authentication. Obviously, it is much easier to deploy a system if all devices share the same encryption key. However, if the key is compromised, the whole system is compromised. Each device should thus have its own encryption key. Managing thousands or even tens of thousands of encryption keys requires an automated enterprise-level solution.

Enterprise-level key management solutions are widely used in some industries, and the technology is even built into systems such as Microsoft® Windows Server®. However, key management solutions are generally tied to specific vendor applications. Standards-based key management exists, but it hasn’t yet made its way to field devices. This will certainly change as DNP3 Secure Authentication becomes more widely used.

Centralized device management is a common requirement in security frameworks, including NERC CIP and the ASAP-SG security profiles. Besides tracking encryption keys, we also will need to keep track of all deployed devices and their configuration.

As vendors identify and address vulnerabilities, they issue firmware updates. The utility will need some automated enterprise-level configuration management application that tracks all deployed devices with their serial numbers, firmware versions, and current settings. The system should have the ability to detect when a device has been replaced or modified, enforce that up-to-date firmware be loaded, and provide the correct configuration settings.
Where do we begin?

We have just briefly skimmed the surface of the subject and have not even addressed critical functions, such as remote access for maintenance. Because everything is now connected and based on programmable devices, engineers will have to take into account new system failure modes resulting from these capabilities.

There is no device that provides all the security controls required to build a secure Smart Grid. A utility undertaking a Smart Grid project will have to work closely with its vendors to ensure that the chosen solution can evolve to meet the requirements outlined above. The lowest-cost device may not be capable of meeting security requirements, even with firmware updates.

A layered approach will need to be used. To meet NERC CIP, utilities have been using security appliances and data concentrators to protect substation devices with little or no security. Similar strategies will need to be used in Smart Grid applications where the cost can be justified.

Utilities should also plan on deploying enterprise-level IED management solutions to provide centralized access control, monitoring, logging, and configuration management functions. It is not practical to track thousands of device serial numbers, firmware versions, and passwords using a spreadsheet.

There is no magic security solution. Building a secure Smart Grid system is a complex engineering project that will require a collaborative effort from all groups involved, from the vendors, the enterprise IT groups, and the engineering teams.

Author

Jacques Benoit is senior product manager and information security analyst in the Energy Automation Solutions business group of Eaton’s Cooper Power Systems.