NERC Critical Infrastructure Protection: Cyber Asset Protection

Rich Hunt
GE Digital Energy, Multilin

1. Introduction

The NERC Critical Infrastructure Protection Committee (CIPC) specifically develops procedural standards related to the protection of the cyber assets within an electric utility. NERC standard CIP-002-1 Critical Cyber Asset Identification requires the identification of critical assets such as control centers, bulk transmission substations, generation resources, load shedding schemes, and special protection systems, and the cyber assets essential to the operation of these critical assets. NERC standard CIP-005-1 Electronic Security Perimeter requires procedures for access request and authorization for communicating to these critical cyber assets, and CIP-007-1 Systems Security Management requires procedures, such as passwords and password management, be in place to prevent unauthorized access to critical cyber assets.

NERC standards are procedural standards, they define the “What” and “Why”, but do not define “How” to implement proper protection of critical cyber assets. As utilities look to implement protection of critical cyber assets, they will look to the suppliers of various cyber assets, such as protective relays, communications equipment, and SCADA systems, to help define and provide solutions for their individual products. In addition, there has been some recent publicity over possible cyber attacks on the utility network, including one specific test (known as the “Aurora test”) where a simulated hacker attack was able to take over the protection and control system of a generator, and physically destroy the generator. CIPC therefore decided to include some equipment suppliers in their discussion around cyber asset protection. A vendor panel discussion was held during the CIPC meeting in December 2007, and included GE Digital Energy among the participants.

The focus of this panel session was the vendor response to a list of questions suggested by utility members of CIPC. Many of the questions directly mentioned the publicized test of the simulated attach on a generator. However, these questions really addressed the basic of cyber asset protection. The questions can be loosely grouped into 3 categories:

- “What should we (the utilities) be concerned about?”
- “What are you (suppliers) doing to help us?”
- “What standards are you trying to meet?”

The rest of this article describes the GE Digital Energy responses to some of these questions.

2. What should utilities be concerned about?

There were several questions from the CIPC members that look for input on suppliers as to the actual cyber asset protection risks that utilities should be concerned about.

If you had to list 5 simple steps for utilities to take to greatly mitigate the Aurora-type vulnerabilities, what would they be?

Implement a security process. Successful security is always procedure driven. Successful procedures always require successful management. The NERC CIP standards directly address this, as they look for documentation on how security procedures are implemented across the utility, as well as the assessment and training of personnel. Without a process, and the management to follow the process, the other steps in security are meaningless.

Identify what needs to be protected. The CIP standards directly describe critical assets, such as generators and bulk transmission substations. A specific asset, such as a generating station, consists of many systems, including the primary generator protection, the excitation system, governor control, primary unit transformer protection, and auxiliary power system. The risks and vulnerabilities of each of these systems must be identified. Each of these subsystems must be addressed in a cyber asset protection plan.

Design for security. The simpler a process, the more reliable the process is. Part of making security procedures simpler is to engineer systems with security in mind from the start. Using a private communications network between sites, such as a SONET network or secure digital radio, prevents public access to your network, greatly reducing exposure and risk. Controlling access to this system, both through authorization and physical control of access points also simplifies security implementation, as does isolating key control networks from public communications networks.

Operate securely. Procedures and design are only as good as the actual operations behind them. Potential cyber attacks are events as significant as regular operational events. Operators must identify and respond to possible cyber attacks. In addition, the monitoring of access to the system, even down to the device level, is necessary. For example, the EnerVista Viewpoint Maintenance software can retrieve a complete security history for GE Multilin relays.

Take simple steps now. Creating security procedures, identifying what needs to be protected, designing for security, and training personnel all take some thought and time to implement. There are simple steps that can be taken immediately. The most basic step is to enable and set passwords in devices that support passwords.

3. What are the top 5 things that a utility should be worried about, and how does Aurora stack up in that top 5?

The Aurora test was an experiment intended to visually make the point that there are threats to the power system. The actions to take, however, are to secure your power system (and generating stations) against the risks based on how your system actually operates. In general, the biggest risks can be seen as:

Malicious physical attack. The electric infrastructure is hard to physically secure and easy to damage. An attack can easily be coordinated across a wide geographic area, targeting difficult to replace transmission assets. Many of these assets, such as large power transformers, and a long mean time to repair, long lead time for replacement, and are custom-designed for each application. The risk is a long-term degradation of the power system.

Unintentional operational mistakes. Employees with authorized access can unintentionally cause events. For example, loading a relay settings file into the incorrect relay can possibly cause protection trips. Good procedures and good system design will help reduce the possibility of operational mistakes, but not all scenarios can be identified or protected against.

Intentional harmful actions by employees. The utility industry has always had examples of disgruntled employees intentionally damaging equipment and the system. This is difficult to protect against, as employees have intimate knowledge of system design and operations, as well as authorized access. The only defense against this is appropriate, attentive management of employees.

Coordinated cyber attacks. The Aurora attack is simply an example of a cyber attack on the power system. Coordinated cyber attacks are difficult to coordinate, and it is possible to detect and defeat these kinds of attacks. There will be evidence of impending attacks, as there must be attempts to locate key assets to attack. However, generating stations are typically more secure against such attacks, due to already implemented security procedures mechanical protection devices, and the presence of human operators at the plant.

4. What is GE Digital Energy doing to help utilities?

The next group of questions directly address how equipment suppliers are helping utilities to address the NERC CIP standards. These questions can be loosely broken down into a couple of basic questions:

- What are you doing to improve or implement security in existing, installed devices, including legacy devices?
- What tools are you developing to help utilities with security management?

Some examples of questions posed by CIPC members to the vendor panel members regarding the Aurora attack are:

There is an Aurora mitigation plan. What are your plans and timeframes for each of the measures that involve you? We want to know what you will do to help mitigate these issues in the installed base of your equipment.

What are you going to do in future firmware upgrades to improve security in the installed base... rather than provide add on products or 'bump in the wire' products or other 'bolt on' solutions.

What are you doing to help companies meet CIP standards and still keep their systems under warranty for both legacy and new systems for patching. Is software "patching" an option for a firmware based device.

[We] have determined the best approach for our substation control IEDs is to use [non-routable] serial communication. Will all of the functions provided via IP communication be available using serial communications? Will serial interfaces continue to be provided for the foreseeable future?

These four questions all relate to support for installed products (modern and legacy) as well as for future installations. The Aurora mitigation plan has many specific requirements, which are simply good security practices. GE Digital Energy already meets much of the requirements of this plan, or is in the process of implementing solutions. These include local and remote passwords in devices, separate passwords for control and setting access, the ability to block access for configuration changes, logging of access to devices, and security audit tools to retrieve access logs. GE Multilin blocks access to all settings in protective relays, not just subsets of settings. Blocking access to all settings reduces the likelihood of unauthorized breaker control, as well as the possibility of malicious setpoint changes.

Fully implementing security measures, especially on installed products, will require firmware updates. GE Digital Energy treats firmware as a product. Each release is a complete, rigorously tested product, using only 1 file to load into an IED. This ensures complete, correct operation of the IED. Patching carries too many risks for incompatibilities and unintentional backdoor access or software hooks to exploit. GE Digital Energy solutions tend to be highly integrated, and we do not promote stand-alone or add-on devices such as communications processors or encryption units.

The challenge is actually updating equipment in the field. This is a time consuming process, and does involve operational risks during the process. Loading new firmware into a line protection relay, for example, typically requires an outage, and a few days of basic protection testing after the new firmware is in place. GE Digital Energy is committed work with customers to help identify which products need to be upgraded, and how best to manage this process. It is important to remember that it may not be possible to upgrade many legacy products due to the performance limitations of processors and hardware.

The question about serial interfaces raises some interesting points. GE Digital Energy will continue to support serial interfaces in our devices as long as there is a market need. Our serial interfaces provide the same access to settings, control, and data that the Ethernet interfaces do. However, the market is moving toward Ethernet due to the advantages of bandwidth, speed, and network availability and redundancy.

Also, serial interfaces are not inherently secure, and in fact, don't address security in any way. Security comes by restricting access to the serial network through other devices. Therefore, security of serial communications and Ethernet communications share the same principles. The best method is to engineer the communications networks with security in mind. Best practices can include:

- Keeping the engineering data access path separate from the SCADA/DCS path.
- Requiring two-step authentication to allow access to change settings, such as explicit permission from system operators.
- Using encrypted communications.
- Controlling physical access to the network, including the use of private networks such as SONET networks between sites.

Independent of the type of communications infrastructure, and the capabilities of installed products, the best solution would be to secure the trunk communications network first. In conjunction, secure installed devices as much as is possible based on their criticality, especially by enabling and using access controls. This greatly reduces the risk of the majority of cyber attack scenarios. This process also is relatively simple, inexpensive, and quick to implement. Going forward, for new projects, security features must be one of the criterion for selecting specific products.

5. Are any of the venders developing software that will assist in dealing with CIP requirements?

The CIP standards had been in development for quite a while before approval. Are your current devices fully compliant with the applicable technical requirements of CIP-005 and CIP-007, especially with respect to access control, monitoring/alerting and logging?

Both of these questions relate to tools to assist utilities in addressing parts of the CIP requirements for monitoring, intrusion detection, and security audit information, and the first one has several interpretations.

Security monitoring tools and intrusion detection tools for the overall communications network are commercially available from information technology suppliers. However, the use of commercial IT tools must be carefully considered as many of these tools assume a large communications bandwidth, and that the data being transmitted is not especially time critical. The communications network, however, is designed to control the power system reliably by issuing time critical controls, often over a network with very limited bandwidth. Security monitoring tools can not disrupt these flow of operational data, or the purpose of the control system, which is reliable operation of the power system, is compromised.

GE Digital Energy does have software tools that can generate and retrieve security audit trail information from a number of our products to facilitate reporting requirements. EnerVista Viewpoint Maintenance automatically retrieves the security log database from protective relays, and automatically generates reports on this database. This information includes changes made to settings, when the changes were made, and the MAC address of the computer that downloaded the settings changes to the relay. This functionality currently exists in a number of GE Multilin protective relays and the software to download and generate audit reports is already commercially available.

6. What standards are you trying to meet?

NERC is a regulatory body, that sets procedural requirements, but NERC is not a standards creating body that sets technical performance requirements. The challenge for electric utilities is to set the technical performance requirements for cyber asset protection in the absence of standards. These next few questions are driving towards how suppliers will be active in standards development.

What are you doing to help companies meet CIP standards and still keep their systems under warranty for both legacy and new systems for: system access and change management – must be controlled much more rigorously than in most companies today? What support is there for centralized authentication and authorization, multi-factor authentication, and access/activity logging? What support is there for configuration management, configuration auditing and change roll-back? How will the system allow autonomous operation in the event that a centralized service (e.g., authorization, logging) is unavailable?

At what point do you feel that 'Certified & Secure by Design' will be available? The real issue is one of complexity & the lack of a "Security Certification" for hardware or an "Underwriters Laboratory" type framework is one of the reasons we see such confusion in the application of security practice & pending compliance.

There are many methods of implementing access and authorization, including centralized authorization, to networks. For example, SONET networks using JungleMux have 3 different ways a user can access the network, all of which have been secured. There is access via the IP network, the optical network, and local serial interface access. All of these methods of access may be available, and all can require a two-step authentication process. So reliability of the cyber security system is very high. The goal of a system that permits access to relays and other IEDs is similar: requiring a two-step authentication process, while the system is highly available to permit the access.

For any type of system to work, there must be an open (non-proprietary), standards-based solution to support this type of access. It quickly becomes unmanageable for vendors, such as GE Digital Energy, and utilities, to have to work towards a variety of different solutions caused by unique interpretations of NERC CIP standards. GE Digital Energy will participate in any such standards development, but this process must be driven by the industry-at-large to be successful.

The concept of Certified and Secure by Design implies there are documented standards that can be designed and tested towards. Such standards must address how passwords are implemented, how authorization is performed, how security audit information is logged, and how these criterions must be met. The CIP standards, as they currently exist, are not precise enough to define what compliance really means. The industry must develop technical performance standards to define compliance, and to define the testing protocols that prove and document compliance. Once again, GE Digital Energy is continually working with NERC, and utilities, and is actively participating in the standards development process, we will ensure our products will comply with these requirements and standards.

7. Conclusions

The electric utility industry is being driven towards implementing cyber asset protection. There is much discussion about what should be done, and how to do it. GE Digital Energy believes that cyber asset protection is essential, and is working to ensure that our products form a sound base for any cyber security plan.

The key to cyber asset protection is more procedural than technical, and requires the identification of critical assets to protect, engineering the control system with security as a key component, operating the system securely, and taking immediate steps to use the existing security capability of products.

GE Digital Energy products already support a wide range of security functions, including:

- Establishment of secure, private communications networks using SONET or digital radio.
- Advanced access control and monitoring, intrusion detection and auditing in our GE Multilin protective relays.
  - Strong passwords, with separate passwords for Local and Remote access to settings and controls.
  - Dual-Permission Access Control to prevent unauthorized setting changes.
  - Access level annunciation and unauthorized access alarms.
  - Security audit logs to keep track of setting changes and commands performed in the relay.
- Secure SONET maintenance access via NERC CIP Security modules in the firmware and VistaNet software for the Lentronics JungleMUX products.
- Advanced network security suite, including SNMP and SYSLOG, in GE MDS wireless technology and products.

For more information, go to www.GEDigitalEnergy.com or contact your local representative.