

Securing the Modern Electric Grid from Physical and Cyber Attacks

Joe Weiss, PE, CISM
Applied Control Solutions, LLC

I appreciate the opportunity to provide the following statement for the record. I have spent more than thirty-five years working in the commercial power industry designing, developing, implementing, and analyzing industrial instrumentation and control systems. I hold two patents on industrial control systems, and am a Fellow of the International Society of Automation. I have performed cyber security vulnerability assessments of power plants, substations, electric utility control centers, and water systems¹. I am a member of many groups working to improve the reliability and availability of critical infrastructures and their control systems.

On October 17, 2007, I testified to this Subcommittee on “Control Systems Cyber Security—The Need for Appropriate Regulations to Assure the Cyber Security of the Electric Grid”².

On March 19, 2009, I testified to the Senate Committee on Commerce, Science, and Transportation on “Control Systems Cyber Security—The Current Status of Cyber Security of Critical Infrastructures”³.

I will provide an update on cyber security of the electric system including adequacy of the NERC CIPs and my views on Smart Grid cyber security. I will also provide my recommendations for DOE, DHS, and Congressional action to help secure the electric grid from cyber incidents.

Background

First of all, I believe it is any utility’s obligation to maintain a high level of electric service reliability. For the most part, the utility industry takes this responsibility very seriously and focuses very strongly on electric system reliability. The grid has been designed to be resilient and accommodate failures (the N-1 criteria). The equipment in place (older legacy and new equipment) has demonstrated a high level of reliability. However, as the older equipment is replaced with new equipment such as for Smart Grid applications an interesting paradox occurs – as reliability increases from the installation of new equipment, the cyber vulnerability also increases.

First, I believe a major point of discontinuity has been the unsuccessful equating of the terms Critical Infrastructure Protection (CIP) and cyber security.

¹ Because much of my information is not in the public domain, I am not at liberty to identify specific utilities on the record.

² http://commerce.senate.gov/public/_files/WeissTestimony.pdf

³ <http://homeland.house.gov/SiteDocuments/20071017164638-60716.pdf>

CIP (or “functional security”) is focused on the function of the electric grid being maintained regardless of the status of the computers. Cyber security, on the other hand, focuses on protecting the computers independent of whether electric reliability is being maintained. For the sake of semantics, I will use the term “cyber security” but my intention is that the operation of the computers is focused on “keeping the lights on,” or what is becoming increasingly referred to as “functional security.”

Secondly, cyber events can be either intentional attacks or unintentional incidents.

NIST defines a cyber incident as “An occurrence that actually or potentially jeopardizes the Confidentiality, Integrity, or Availability (CIA) of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies. Incidents may be intentional or unintentional.”⁴

Cyber incidents are also more than just malware or botnet attacks. Cyber incidents include all forms of impacts on electronic communications.

Man-made Electromagnetic Interference (EMI) has already impacted North American and European electric and water Supervisory Control and Data Acquisition (SCADA) systems and ruptured a natural gas pipeline.

In industry control systems, the most probable cyber incident is unintentional. Moreover, in a stellar application of the “law of unintended consequences,” I believe that “blindly” following the NERC CIPs⁵ will result in more unintentional cyber incidents.

Unintentional cyber incidents have already killed people, caused significant outages, and large economic impacts. Additionally, if the incident can be caused unintentionally, the same type of incident, if intentional, could have even more damaging effect.

Recent History

What has been happening since I testified to this Subcommittee in October 2007? It is not a pretty picture and the power industry clearly needs Congress’s help.

Knowledge Base - Figure 1 characterizes the relationship of the different types of special technical skills needed for control system cyber security expertise, and the relative quantities of each at work in the industry today.

Most people now becoming involved with control system cyber security typically come from a mainstream business Information Technology (IT) security background and not a control system background. This trend is certainly being accelerated by the Smart Grid initiatives, where the apparent lines between IT and control systems are blurring. Many of the entities responsible for control system cybersecurity, industry, equipment

⁴ FIPS PUB 200, *Minimum Security Requirements for Federal Information and Information System*, March 2006.

⁵ <http://www.nerc.com/page.php?cid=2|20>

suppliers, and government personnel (e.g., DHS NCSD and S&T, DOE, EPA, etc.) do not entirely appreciate the difficulties created by this trend.

This lack of appreciation has resulted in the repackaging of IT business security techniques for control systems rather than addressing the needs of field control system devices that often have no security or lack the capability to implement modern security mitigation technologies. This, in some cases, has resulted in making control systems less reliable without providing increased security. An example of the uninformed use of mainstream IT technologies is utilizing port scanners on Programmable Logic Controller (PLC) networks. This has the unintended consequence of shutting them down. This specific type of cyber incident has occurred more than once in both the nuclear power and conventional power portions of the industry, with negative consequences.

As can be seen in Figure 1, IT encompasses a large realm, but does not include control system processes. Arguably, there are less than several hundred people world-wide that fit into the tiny dot called control system cyber security. Of that very small number, an even smaller fraction exists within the electric power community.

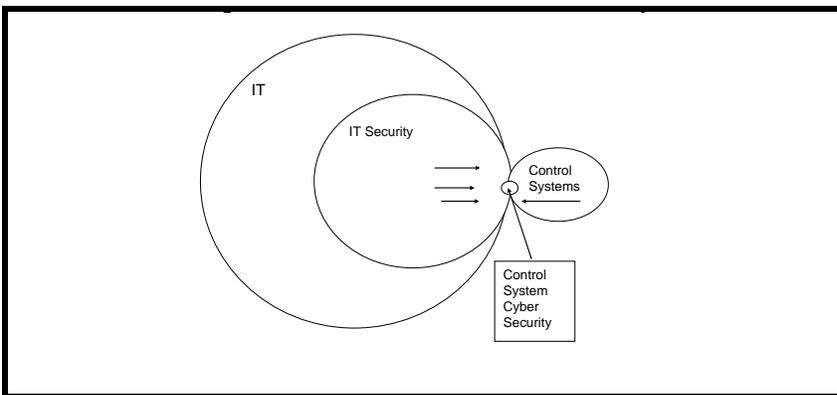


Figure 1 - Relationship and Relative Availability of Control System Cyber Security Expertise

Control System Cyber Incidents - Since I testified to this Subcommittee in October 2007, I have documented more than 30 control system cyber incidents, **more than 20 of which were in the North American electric power industry!** These incidents affected nuclear and fossil plants, substations, and control centers. Impacts ranged from loss of displays, controller slowdowns and shutdowns, plant shutdowns, and a major regional power outage. Geographically, these incidents occurred in more than ten states and a Canadian province. None of the incidents were actually identified as “cyber”.

Meeting the NERC CIPs would not have prevented many of these incidents. In fact, some could have actually been caused or exacerbated by following the NERC CIPs.

Equipment Suppliers – It is important to understand that suppliers provide equipment with the features their customers’ request. Given that fact, the report card on our control system suppliers is a mixed bag. Responding to industry requests, the major Distributed Control System (DCS) and SCADA suppliers have been addressing security at the master station level. However, suppliers of field control and equipment monitoring systems have not had those industry requests and thus are continuing to include dial-up or wireless modems, Blue Tooth and Zigbee connections, and/or direct Internet connections as part of their product offerings. This also applies to equipment used in the Smart Grid and nuclear plants.

Business IT-focused suppliers continue to supply equipment and testing tools designed for IT applications not for legacy control systems applications. This has resulted in control system equipment impacts including shutdown or even hardware failures.

Consultants and System Integrators – Most of the consultants and system integrators that are focusing on “cyber security” are really focusing on compliance for NERC CIPs. Most are focusing on the SCADA or DCS master stations as they are IT-like systems that non-control system personnel can understand. That leaves the legacy field equipment that has essentially no security hardly even addressed as part of the NERC CIP process. The consultants and system integrators that are focused on equipment upgrades or new equipment installation generally do not address security.

Utilities – The original intention of the NERC CIPs (even before they were called the CIPs) were to make the bulk electric grid secure. Unfortunately, the “letter of the law” of the NERC CIPs is not security, but compliance. It is a critically important distinction to make, and to understand. I know of only one utility that is trying to assure their systems are secure independent of compliance considerations. Almost all utilities are playing the game of compliance rather than securing their systems. This has resulted in industry’s lukewarm attempt to meet NERC Advisories such as Aurora⁶. This lack of will has directly led to the significant number of actual electric industry cyber incidents many of which were not even addressed by the NERC CIPs!

NERC – The North American Electric Reliability Corporation (NERC) was established in 1968 to ensure the reliability of the bulk power system in North America. NERC is a self-regulatory organization, subject to oversight by FERC and governmental authorities in Canada. As of June 18, 2007, FERC granted NERC the legal authority to enforce reliability standards with all US users, owners, and operators of the bulk power system, and made compliance with those standards mandatory and enforceable making NERC the Electric Reliability Organization (ERO). NERC’s status as a self-regulatory organization means that it is a non-government organization which has statutory responsibility to regulate bulk power system users, owners, and operators through the adoption and enforcement of standards for fair, ethical and efficient practices.⁷ Prior to becoming the ERO, NERC was an American National Standards Institute (ANSI)-accredited organization meaning it was a consensus standards organization and was subject to the

⁶ <http://homeland.house.gov/SiteDocuments/20080521142118-53954.pdf>

⁷ <http://www.nerc.com/page.php?cid=1>

direction of its member utility organizations. The ANSI accreditation requires standards need to go through a formal ballot process. This is a time-consuming effort and tends to favor setting a “very low bar.” This consensus process has resulted in cyber security standards that are very weak and ambiguous assets *and even exclude some of the most important recommendations from the Final Report of the Northeast Outage*⁸. In the past, NERC has been a clear obstructionist to adequately securing the electric grid. NERC has used the ANSI process to reject more comprehensive requirements. That obstructionism included public responses denigrating Project Aurora⁹. The consensus approach is adequate for subjects like tree-trimming but is not appropriate for critical infrastructure protection.

I was part of the NIST/MITRE team that performed a line-by-line comparison of the NERC CIPs to NIST Special Publication (SP) 800-53¹⁰ which is mandatory for all federal agencies including federal power agencies¹¹. The report demonstrates that NIST SP800-53 is more comprehensive than the NERC CIPs. However, NERC and many utilities are fighting the implementation of NIST SP800-53. Are the utilities trying to say that the computers at the Department of Housing and Urban Development need a more comprehensive set of cyber security rules than every non-federal power plant, substation, and control center in the United States? Unless an asset is classified as “critical” in CIP-002, no further cyber security evaluation is necessary. A large segment of the utility industry is using the amorphous requirements in CIP-002 to exclude most of their control system assets from even being assessed. Michael Assante, Vice President and Chief Security Officer of NERC wrote a public open letter on April 7th¹² in which he makes it very clear that the industry is not doing an adequate job of even meeting the weakened intent of the NERC CIPs. Specifically, Assante’s letter states that only 29 percent of Generation Owners and Operators identified at least one Critical Asset and fewer than 63 percent of the transmission owners identified at least one Critical Asset. This means that 71% of generation owners did not identify a single critical asset and 37% of transmission owners did not identify a single critical asset. I am personally aware of utilities that have identified ZERO Critical Assets even though they have automated their plants and substations and have control centers.

Despite Assante’s attempts to change NERC’s approach on cyber security, NERC has continued its focus as a utility-directed organization. NERC’s Board of Trustees approved revisions to the NERC CIPs on May 6, 2009 after passage by the electric industry with an 88 percent approval rating. However, the revisions did not address any of the technical limitations such as exclusions of telecom, distribution, non-routable protocols or strengthening CIP-002 to address Assante’s April 7th letter. A second example would be the June 30, 2009 Alert on the Conficker Worm.¹³ The Alert states the

⁸ <https://reports.energy.gov/BlackoutFinal-Web.pdf>

⁹ <http://www.cnn.com/2007/US/09/27/power.at.risk/index.html>

¹⁰ <http://csrc.nist.gov/publications/PubsDrafts.html#SP-800-53-Rev.%203>

¹¹ Marshall Abrams, MITRE Technical Report, MTR70050, Addressing Industrial Control Systems in NIST Special Publication 800-53, March 2007.

¹² Letter from Mike Assante to NERC Industry Stakeholders, “Critical Cyber Asset Identification”, April 7, 2009

¹³ <http://www.nerc.com/page.php?cid=5%7C63>

ES-ISAC estimates the risk to bulk power system reliability from Conficker is LOW due to the limited exploitation of this vulnerability and generally widespread awareness of the issue even though NERC acknowledges the potential consequence is high and the awareness among control system users is very low.

Smart Grid – The intent of the Smart Grid is to embed intelligence into the electric grid to allow two-way communications between devices and control centers for monitoring and control. The Smart Grid’s use of the Internet and Internet Protocols (IP) is blurring the line between business IT and control systems resulting in more people without knowledge of the electric system being involved in securing these systems.

This is a recipe for disaster - there has already been at least one case of a denial of service attack (DDOS) to a distribution automation system.

From a Regulatory standpoint, the situation is convoluted because the NERC CIPs explicitly exclude electric distribution which is the heart of the Smart Grid and yet the NIST Smart Grid security efforts point to the NERC CIPs.

Unless Congress passes legislation to allow FERC to include distribution or the individual public utility commissions mandate that the NERC CIPs must be followed for their distribution systems, there are no regulations for securing the Smart Grid.

Education – To the best of my knowledge, there are no technical, interdisciplinary university curricula for control systems cyber security. There are universities starting to address this subject in an ad hoc manner such as the University of Illinois and Mississippi State University. Congress might well seek ways to encourage and fund more such curricula as a significant way to improve cyber security in all control systems.

Certifications – There are no personnel certifications for *control system* cyber security.

IT certifications such as the Certified Information Systems Security Professional (CISSP) and the Certified Information Security Manager (CISM) do not address control systems. Professional engineering examinations do not include security.

There needs to be a certification demonstrating knowledge of control systems as well as security by organizations competent to oversee this requirement. One organization could be the CSFE¹⁴ which certifies Functional Safety experts. There are on-going efforts by individual companies and organizations such as ISA to certify industrial control systems for cyber security.

Government R&D – R&D has been focused on effectively “repackaging IT”. Very little work has been devoted to legacy and even new field equipment, even though these devices have limited or no security, and can cause the biggest impacts.

¹⁴ www.csfe.org

There has also been no attempt to analyze actual cyber incidents to learn what policies and technologies should be developed to protect them.

NIST – NIST has effectively two disjointed programs on cyber security that impact the electric grid. The NIST Information Technology (IT) Laboratory has been responsible for updating NIST SP800-53 and the daughter standard NIST SP800-82¹⁵. There has been a significant amount of effort addressing industrial control systems and applicability to the electric industry. NIST is also acting as the standards coordinator for the Smart Grid.

As a member of the Smart Grid Cyber Security Working Group and the Industry-to-Grid Working Group, I see a dichotomy that troubles me. Instead of mandating NIST SP800-53 for the Smart Grid, it appears as if NIST doesn't want to be seen as pushing their own standards. Not only is NIST SP800-53 the best cyber security standard currently available, it is mandatory for all federal power agencies.

Why shouldn't NIST SP800-53 be mandated for all power utilities, not just federal ones?

Recommendations

Traditional reliability threats such as tree trimming to prevent power line damage could be handled by private industry. However cyber is a new threat that requires a joint effort by the government and private industry. I believe there are a number of roles for the federal government to play in defending against cyber incidents and/or physical attacks against electric facilities.

Articles such as the recent Wall Street Journal article on Chinese and Russian hackers imply that the electric industry is unaware of computer intrusions¹⁶. This is probably true on several accounts. As mentioned, the electric industry is not doing an adequate job of even looking. Additionally, there is a lack of adequate cyber forensics for control systems. This leads to the fact that it is difficult to have an early detection and warning capability for cyber threats for the electric industry today. However, that same difficulty is also an opportunity for the government and private industry to develop appropriate forensics. A non-technical challenge is the industry's continuing reticence to provide control system cyber incident data to the government and for law enforcement to share relevant information on actual attacks to the industry so they can protect themselves.

What can DHS and DOE do?

I cannot speak for the division in responsibilities between DHS and DOE, but I can point out what needs to be done:

- Provide intelligence on threats to those needing to know - that does not mean only security cleared individuals, but all individuals working in the area;

¹⁵ http://csrc.nist.gov/publications/drafts/800-82/draft_sp800-82-fpd.pdf

¹⁶ <http://online.wsj.com/article/SB123914805204099085.html>

- Make use of available technical talent – there is very little, and the safety and security of our country depend on these efforts;
- Analyze actual control system cyber incidents to develop appropriate cyber technologies and policies – there are few places to get the information as most of it has not been provided to the government—and what has is often classified and unavailable;
- Establish benchmarks for how much security is enough, what is an acceptable vulnerability assessment, what is an acceptable risk assessment, audit metrics, trade-offs between security and functionality, etc.;
- Support first-of-kind technology development, particularly for legacy field devices;
- Support development of college technical as well as policy curricula;
- Support the establishment of a CERT (Computer Emergency Response Team) for control systems that is not under the purview of the government, because industry is still uncomfortable about providing what they consider to be confidential data to government agencies like the FBI.

What can Congress do?

Currently **FERC** is constrained by the Energy Policy Act of 2005¹⁷. It cannot write standards and its scope is restricted to the bulk electric system. There are several steps that Congress can take to help maintain the reliability of the electric system from cyber threats:

Comment [MDA1]: No introduction. You need to build up FERC.

1. Provide cyber security legislation that gives FERC the scope to write standards including mandating NIST SP800-53 for the bulk electric grid and the Smart Grid
2. For cyber security, increase FERC’s scope to include electric distribution. There are technical as well as administrative reasons. Low voltage transmission and high voltage distribution systems electronically communicate with each other; utilities electronically communicate with each other; and the utilities use common systems. We cannot afford to have a “Tower of Babel” set of rules for each state and for the same equipment.
3. NERC is in a conflict-of-interest position because its fundamental purpose has changed. If NERC can not do the job of assuring cyber security of the electric grid, find an organization with the will power and authority to do so.
4. HR 2195¹⁸ would go a long way toward providing effective legislation. I would add the following: Mandate the NIST FISMA guidance documents, such as SP800-53 and require the establishment of a program to develop expertise in electric grid cyber security. The expertise gained from this program should be shared with every electric grid owner and operator.

Summary

It has been almost ten years since I helped start the control system cyber security program at the Electric Power Research Institute (EPRI). Ten years should have been sufficient

¹⁷ http://en.wikipedia.org/wiki/Energy_Policy_Act_of_2005

¹⁸ <http://www.opencongress.org/bill/111-h2195/text>

time for the industry to make significant progress. Unfortunately, it has not happened. Actual control system cyber incidents continue to occur – in fact, they appear to be getting more numerous. An unsecured electric grid is dangerous to the safety and economic well-being of this country. Congress needs to step in and provide regulation to give FERC the additional powers necessary and mandate NIST SP800-53.