The Past, Present, and Future of Securing Electric Power Systems
Jonathan Pollet, Industrial Defender

Abstract
This paper first provides a look back at the last 10 years of security events that have shaped the electric power industry, then it provides a commentary on the current state of security in the North American Electric Utility sector. This paper does not only point out the issues, but also concludes with practical information on how to physically and electronically secure electric power systems. These solutions are future-proof, meaning that investments made in these categories will not only comply with current NERC CIP requirements, but will continue to secure power systems into the future as the standards continue to evolve. The content in this paper is the result from performing over 90 security assessments and architecture design projects specifically for securing electric power systems.

1. Introduction

If you were to look at the interconnections and electronic protocols used for operation and control of the North American Electric Power Grid, it would look different today than it did just 10 years ago. Upgrades from older RS-232 and serial-connected systems to new protocols based on TCP/IP and routable commands, plus the increased need to connect the control room systems to business and IT networks, creates a new emergence of cyber threats to this ecosystem. In addition to the growing cyber security issue, physical security is also a concern as more remote sites change from manned to un-manned locations. Some of the most critical interconnections and ties are done in switchyards that are essentially lights-out operations. This paper first provides a look back across 10 years of security incidents and events that have occurred in the electric power industry, then discusses the current state of the cyber and physical security of the North American Electric Power System, as seen from over 90 security assessments of critical infrastructure systems. This paper then provides practical solutions for securing these systems, which can be implemented to meet the NERC CIP compliance requirements.

2. The Past - 10 Years of Security Events that have Shaped the Electric Power Industry

To properly understand the current status of the US and Canadian Power Infrastructure, it helps to understand the history of incidents and events that have shaped the need for increased physical and cyber security controls.

Security issues with the North American critical infrastructure were not just the concern of security researchers, consultants, and those studying this problem. The awareness of the issue also had visibility within the US Government, and on July 15, 1996, the Executive Order EO 13010 for Critical Infrastructure Protection was established so that government and the private sector would begin to work together to understand the physical threats to tangible property ("physical threats"), and threats of electronic, radio-frequency, or computer-based attacks on the information or communications components that control critical infrastructures ("cyber threats"). [1]

In October of 1997, the President's Commission on Critical Infrastructure Protection issued its report, "Critical Foundations: Protecting America's Infrastructures." It called for a national effort to assure the security of the United States' increasingly vulnerable and interconnected infrastructures, such as telecommunications, banking and finance, energy, transportation and essential government services. In response to this report, the Presidential Decision Directive 63 was initiated as an interagency effort to evaluate those recommendations and produce a workable and innovative framework for critical infrastructure protection. This directive, PDD 63, was released in May of 1998, and called for a national center to warn of and respond to attacks. The declared goal was to ensure the capability to protect critical infrastructures from intentional acts by 2003. [2]

In the summer of 2001, the coordinator for the city of Mountain View, Calif.'s Web site noticed a suspicious pattern of intrusions. The FBI investigated and found similar "multiple casings of sites" in other cities throughout the U.S. The probes were seemingly emanating from the Middle East and South Asia, and the Visitors were looking up information about the cities' utilities, government offices, and emergency systems. This information took on a new significance when U.S. intelligence officials examined computers seized from Al Qaeda operatives after the Sept. 11
attacks and discovered what appeared to be a broad pattern of surveillance of U.S. infrastructure. [3]

The August 14, 2003 blackout was the next reminder to the industry of how interconnected the North American Electric Grid is, and how a vulnerability in one system at one company can have cascading effects on an entire region. In chapter 9 of the Final Report from the US-Canadian Task Force that reviewed the causes and results of the blackout, the report states: “...there are potential opportunities for cyber system compromise of Energy Management Systems (EMS) and their supporting information technology (IT) infrastructure. Vulnerabilities were observed in some facilities, such as unnecessary software services not denied by default, loosely controlled system access and perimeter control, poor patch management, and poor system security documentation.” [4]

Less than a week after the blackout, on August 19, 2003, the Slammer worm penetrated a private computer network at Ohio’s Davis-Besse nuclear power plant and disabled a safety monitoring system for nearly five hours. According to an industry report, the same worm downed a utility’s critical SCADA network after penetrating a control center network through a VPN connection, and, separately, disrupted a power company’s SCADA traffic by consuming bandwidth on a shared facility.

In 2004, NERC (then called the North Electric Reliability Council), voted to renew the Urgent Action Cyber Security Standard 1200, but these standards did not have any required mandates or regulations behind them, and the electric utility industry at large acted slowly to implement the minimum suggested recommendations.

By early 2005, FERC stepped in and recommended to NERC that a new mandatory standard, to be called NERC 1300, supersede the voluntary 1200 urgent action, and made it clear that federal regulations would be enacted and enforced if the industry organization did not take action on a voluntary basis.

The new Energy Policy Act of 2005 was voted on and approved in the US that addressed many goals to improve the strategic posture of the United States in Energy sectors such as Natural Gas and Hydropower. The most interesting outcome of this new Energy Act, in terms of the security of the electric grid, was the authority that this act gave to FERC to approve new electric sector security standards, and mandate its compliance through penalties and fines for those under its jurisdiction, which included: owners, operators, users of the bulk electric power system, including state and municipal entities, and rural cooperatives. Soon after the release of this new Energy Act of 2005, FERC named NERC as the one responsible ERO (Electric Reliability Organization), and empowered NERC with the task of finalizing the new Cyber Security standards. More importantly, this included the ability to audit and levy fines.

The new NERC 1300 standard, which was renamed the NERC CIP Cyber Security Standards, and by May of 2006, draft 4 was ratified and approved by the NERC drafting committee. The NERC drafting board submitted draft 4 to FERC on August 28, 2006 with standards 002 through 009. It outlined minimum requirements for physical and cyber security controls and provided timelines for when electric utilities should BW (begin work), become SC (substantially compliant), C (compliant), and AC (audit-ably compliant). Most utilities were to begin implementing the standards in 2006, and be ready for audits to begin in 2010.

Throughout the rest of 2006 and 2007, many utilities took a “wait and see” approach to the new NERC CIP standards, and there was concern that FERC would not approve the NERC CIP draft 4 standards. Several utilities that we worked with indicated that they were going to wait to see what comes out of the FERC NOPRs, and also look to see what their industry peers were doing before committing to a capital-intensive security overhaul. As a cyber security services and product provider, we saw a slight increase in the number of RFPs (request for proposals) hit the market in 2007, and it seemed that the rate of adoption of these NERC CIP standards was slower than anticipated in the market.

On January 17, 2008, FERC approved the NERC CIP Cyber Security Standards, and compliance to these standards became mandatory and enforceable by federal law, backed with fines and penalties for non-compliance. Shortly after this, we began to see the cyber security market flooded with requests for security consulting services to help utilities respond to these mandatory standards, as well as requests to pilot security products and technology used to secure their control room and remote locations.

Whereas in the past, the electric power industry could implement whatever level of physical and cyber security controls they deemed necessary to mitigate their risk, the NERC CIP standards forced at least a minimum set of physical and cyber controls across the entire bulk electric supply system.

Meanwhile, while the electric power industry was busy assessing their compliance gaps and implementing new controls to mitigate their risks, threats to the system continued to appear. In January of 2008, in New Orleans, US Central Intelligence Agency senior analyst Tom Donahue told a gathering of 300 US, UK, Swedish, and Dutch government officials and engineers and security managers from electric, water, oil & gas and other critical industry asset owners from all across North America, that “We have information,
from multiple regions outside the United States, of
cyber intrusions into utilities, followed by extortion
demands. We suspect, but cannot confirm, that some of
these attackers had the benefit of inside knowledge.
We have information that cyber attacks have been used
to disrupt power equipment in several regions outside
the United States. In at least one case, the disruption
cause a power outage affecting multiple cities. We do
not know who executed these attacks or why, but all
involved intrusions through the Internet." [5]

A few months later, on March 7, 2008, a nuclear
power plant in Georgia was forced into an emergency
shutdown for 48 hours after a software update was
installed on a single computer. The computer in
question was used to monitor chemical and diagnostic
data from one of the facility's primary control systems,
and the software update was designed to synchronize
data on both systems. According to a report filed with
the Nuclear Regulatory Commission, when the updated
computer rebooted, it reset the data on the control
system, causing safety systems to errantly interpret the
lack of data as a drop in water reservoirs that cool the
plant's radioactive nuclear fuel rods. As a result,
automated safety systems at the plant triggered a
shutdown. This was not a direct attack on an element
of the North American Electric Power System, but was
an indication and verification that the control room and
remote substation networks are still connected to
business IT networks, and internal vulnerabilities can
be triggered by either external or internal agents that
can cause outages. [6]

Table 1 below shows a timeline of the events
mentioned in this section, and provides a history of
incidents and events that have shaped the need for
enhanced security in electric power systems in the US
and Canada.

<table>
<thead>
<tr>
<th>Date</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>July 15, 1996</td>
<td>Executive Order EO 13010 for Critical Infrastructure Protection established to understand the physical and cyber threats to the US critical infrastructure.</td>
</tr>
<tr>
<td>May 22, 1998</td>
<td>President Clinton warned, “Intentional attacks against our critical systems are already under way,” and created the Presidential Decision Directive 63 to create a framework for critical infrastructure protection.</td>
</tr>
<tr>
<td>Aug 14, 2003</td>
<td>August 2003 blackout showed potential opportunities for cyber system compromise of Energy Management Systems (EMS) and their supporting information technology (IT) infrastructure.</td>
</tr>
<tr>
<td>Aug 19, 2003</td>
<td>Slammer worm penetrated a private computer network at Ohio's Davis-Besse nuclear power plant and disabled a safety monitoring system.</td>
</tr>
<tr>
<td>2004</td>
<td>NERC votes to renew Urgent Action Cyber Security Standard 1200, but with no mandatory compliance.</td>
</tr>
<tr>
<td>Feb 3, 2006</td>
<td>FERC commissions NERC to develop the reliability standards.</td>
</tr>
<tr>
<td>Dec 11, 2006</td>
<td>FERC issues its assessment of the proposed standards and ask for comments on them, due in February</td>
</tr>
<tr>
<td>Feb 12, 2007</td>
<td>NERC begins addressing comments on the proposed standards</td>
</tr>
<tr>
<td>Jul 20, 2007</td>
<td>FERC proposes to approve the revised standards and gives the community until October 5, 2007 to comment</td>
</tr>
<tr>
<td>Aug 6, 2007</td>
<td>18 CFR Part 39 is filed on the Federal Register as a proposed rule.</td>
</tr>
<tr>
<td>Jan 17, 2008</td>
<td>FERC approves NERC-CIP standards.</td>
</tr>
</tbody>
</table>
| Jan 17, 2008 | CIA discloses at SANS event in New Orleans that they have information, from multiple regions outside the United States, of cyber intrusions into utilities, followed by extortion demands. They also disclosed information that cyber attacks have been used to disrupt power equipment in several regions outside the United States.
Table 1 - Timeline of Recent Security Incidents and Events in the Electric Power Industry

<table>
<thead>
<tr>
<th>Date</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mar 7, 2008</td>
<td>Nuclear power plant in Georgia was forced into an emergency shutdown for 48 hours after a software update was installed on a single computer. Interconnections and dependencies between business IT computers and control system resources sited as the cause of the shutdown triggered by the safety system.</td>
</tr>
</tbody>
</table>

3. The Present - Current Physical and Cyber Security Findings

The past 10 years of security events provides good context for understanding how the physical and cyber security controls in the electric power industry have changed from some of the initial security assessments performed in 2002 through some of the more recent findings in 2008.

3.1 Overview of Physical Security Findings

In some of the early security assessments from 2002 through 2005, our security services team could almost always find at least a dozen physical security findings that we considered “low-hanging fruit” - meaning that these were issues that were relatively simplistic to resolve and were low-to-medium cost to resolve. Many of these early physical security issues were iterations of the following general findings:

- propped open doors
- unlocked doors
- poorly maintained perimeter fencing
- critical cyber devices in plain sight
- critical cyber devices accessible by all
- lock boxes for all facility keys in plain sight
- loose perimeter controls
- lack of monitoring
- failure to maintain access logs
- lack of surveillance
- lack of security awareness training
- poorly maintained written policies/procedures
- incident response plans not documented
- lack of coordination with local law enforcement
- deficiencies in emergency response planning

As the industry evolved, and physical and cyber security became a more prevalent topic at meetings, in the media, and within the electric power industry, we found that the physical controls were the first area to improve. The NERC 1200, 1300, and CIP standards that emerged, while mainly covered cyber security requirements, did require utilities to physically secure access to critical cyber assets and monitor and log access to these systems. This meant that utilities had to start thinking about how to physically secure access to network equipment, computer workstations, servers, and embedded devices like RTUs (remote terminal units) and IEDS (intelligent electronic devices). They also had to start thinking about how to monitor and log physical access to these devices.

Recently, our security services team has seen a recent increase in the level of physical security implemented to secure access to control rooms and remote substations, and the NERC CIP standards have been a change agent responsible for some of the increased security. The other change agent is the price of copper and metals. Over the past several years utilities have had an increase in the theft of spare copper wire and equipment due to the high demand for these metals in the market. Several utilities that we have worked with have indicated that they have upgraded their perimeter fencing, upgraded their locks, and installed monitoring and surveillance systems to alert them to unauthorized access attempts at remote unmanned facilities. While these upgrades are a part of the NERC CIP compliance requirements, several utilities sited their real reason for upgrading their physical security has been to limit their loss of copper wire, aluminum wire, and other spare parts and equipment, typically stored inside substation yards.

3.2 Overview of Cyber Security Findings

It is probably no surprise that the trend on the cyber security side reflects similar findings as seen on the physical side. Just as with physical security, the cyber security controls were loose early from 2002 through 2005, and it was very typical for security assessment teams to find security issues starting from the perimeter of the SCADA or EMS systems, down throughout the network infrastructure, as well as in the computer operating system layer, application layer, SCADA protocol interconnections, and even with the embedded RTU and IED devices. By 2006, there were several “top 10 vulnerability” lists starting to appear, with the Department of Energy, National Labs, and several private commercial firms all indicating cyber security gaps in the following areas:

- inadequate policies, procedures, and training
insufficient separation between business IT and control system networks
insecure remote access through dial-up and TCP/IP connections
network devices not on current firmware
improper configuration of firewalls/routers
use of clear-text protocols like TELNET, FTP
inadequately secured wireless systems
lack of hardening in workstation and server OS
lack of patch management process
default OS and application logins and passwords
inappropriate applications on SCADA/EMS computers
failure to enable logging on network devices, computing resources, and embedded devices
lack of network monitoring, and failure to alert on abnormal system conditions
lack of centralized logging / alerting solution
lack of trained security personnel to maintain security patches, signatures, and to perform basic system administration
failure to maintain accurate system drawings and documentation

Just as with physical security, as the industry evolved, the level of cyber security hardening increased, and from 2006 through the present, our security services team are finding that the power utility industry as a whole is implementing more cyber security controls, and are also providing more access to training and tools to the people responsible for securing the SCADA and EMS systems. We are seeing a trend in the timing of security services demand and product implementations. Since most utilities can not implement all of the services and products that they need in one budget year, most seem to be spreading their security budgets over 3 or more years, and the typical pattern emerges:

1. Utilize internal and external consultants to perform an assessment of the current security posture, and to prioritize where to focus their activities in securing their infrastructure. Sometimes this assessment may also focus on what gaps the utility has in their NERC CIP Compliance efforts.
2. Once an assessment or gap analysis is performed, most then start their mitigation strategy with securing the perimeter between their business IT and SCADA/EMS systems. This has also been called a network architecture or network segmentation project.
3. The next area of focus most utilities are concerned about is the remote access to their SCADA, EMS, and Control Systems. This is a major issue with vendors, external contractors, and internal technicians all wanting remote access. Best-in-breed solutions incorporate both dial-up as well as TCP/IP access under the same technology utilizing 2-factor authentication, and often leveraging the corporate active directory authentication scheme.
4. The next wave of spending, once the perimeter and remote access issues are resolved tends to be implementing a centralized logging, monitoring, and alerting system for their network infrastructure
5. Once the centralized event monitoring and alerting system is up and running, many utilities are looking to extend this solution deeper into the operating systems and applications running on their computer workstations and servers, and then eventually to all critical cyber assets, so that eventually all CCAs (critical cyber assets) are being monitored and are sending their logs to one centralized system.
6. Monitoring and logging alerts to a centralized solution is only half of the problem, and typically only tells the system administrator what happened after it already happened on the system. While most utilities are using SNMP and SYSLOG compatible solutions for achieving this forensic benefit, most still see the need for an IDS/IPS solution that can more quickly identify potential intrusions and prevent them at the perimeter. Due to the sensitivity of SCADA, EMS, and Control Systems, IDS should only be used at the edge or perimeter of the network. We have seen though where IDS solutions, both network-based (NIDS) and host-based (HIDS) are being deployed further down into the SCADA, EMS, and Control Systems architecture. Some HIDS software agents also detect and alert on changes to the host, which helps comply with the ports/services, admin account, and change control monitoring requirements in the NERC CIP-007 requirements.

4. The Future - Building Out a Future-Proof Security System

Given the interesting incidents and events that have shaped the security posture of the electric utility industry, and knowing what are the current requirements and trends in physical and cyber security, we can then start to see what a total solution might look like that would not only comply with the current NERC CIP standards, but also stand up to any twists and changes to these standards in the future.

It does not take any magical powers or a crystal ball to see where the future is going with cyber security, and if we consider the potential attack surface and threat vectors that could disrupt SCADA, EMS, and...
Control Systems, we can design a system of solutions that not only comply with the NERC CIP standards today, but also protects that investment into the future.

The best way to envision or design a security system is to start by thinking about the type of threats that this system should defend against. The solutions should be built to ensure that it can defend both current threats, attack surface, as well as new potential vulnerabilities. It should be flexible to be easy to be updated so that the threats of tomorrow can be quickly identified, prevented, and the right personnel can be notified to take action. The topic of convergence of physical and cyber security should be covered in another future paper. For the purposes of this paper, we will focus on cyber security systems as we take a look at security systems that can be made future-proof.

Cyber security solutions are most simplistically broken down into providing the following types of functions:

1. **Active Defense (blocking)**
   - Routers/Firewalls/UTMs (network segmentation)
   - IPS / Antivirus / Malware Prevention (could be network and/or host-based)

2. **Passive Detection (detect/log/alert)**
   - NIDS (network)
   - HIDS (host)
   - Monitoring (SNMP)
   - Log Management (SYSLOG)
   - Alert Correlation & Escalation (Incident Response / Forensics)

3. **System Administration (admin)**
   - Secure Remote Access
   - User Authentication / Identity Management
   - Security Update Management (Signature/Firmware Management)
   - Document/Configuration Management
   - Change Management

When evaluating cyber security solutions, ask the tough questions, and see how the proposed solution accomplishes those above three basic functions of active defense, passive detection, and system administration. The evaluation process should also involve ensuring that the vendor is using secure coding practices, has a robust quality assurance and testing procedure for all products, and has vetted their employees through effective background checks. Some of the largest security breaches in the past were accomplished by planting individuals into organizations on the front-end during the software development cycle. This allowed back-doors to be hard-coded into the software and hardware. The responsibility for personnel risk assessments and personnel training is also shared by the end users of the security systems, as indicated and required by several areas of the NERC CIP and ISO 270001 standard. Although much of the attention is focused on the technical abilities of the software and hardware solutions, we should always pay attention to the people aspect of security, and the risk of the insider threat.

It was a prior best practice to select individual components that were considered “best-in-breed” then use open source software and internal software development to “glue” all of the pieces of a cyber security solution together into one system. That mindset is no longer considered best practice because it raises the overall total cost of ownership due to having to maintain various firmware, signatures, and application versions across diverse vendors. It can create areas of overlap where the functionality of one system stops and the next security component starts. Piecing together a security solution from multiple vendors can also create a situation where each of the vendors are all pointing fingers at each other if the various components do not interoperate effectively.

For these reasons, it is important to try to select a vendor that has most of the requirements mentioned above covered with one system, then qualifies other interoperable 3rd party solutions through a certified partner program so that the guess work is eliminated and the risk is lowered for the end user. It is also a good practice to test, or pilot the solution on a small scale, then build out the solution across all critical assets, once the system meets performance and security requirements.

It goes without saying that a solid security policy framework is also necessary for a strong security program. Since the NERC CIP standards contain vague and nebulous language, and will continue to change under the direction of FERC and the NERC drafting committee, it may be necessary to look to other more prescriptive security frameworks like the NIST 800-53 or the ISO 270001.

All of the NERC CIP security controls can be found and mapped to existing controls in both the NIST 800-53 and ISO 270001, but the reverse is not true. The advice for any organization wishing to “future-proof” their security program, would be to look towards these more robust and prescriptive security frameworks for the basis for the security controls, policies, and procedures that govern the operation, administration, and maintenance of the security program of the future.
5. Summary

It is important to understand the events that have transpired over the past 10 years that helped shape the security posture of the electric power industry. This provides the context needed to then discuss the general status of the industry’s physical and cyber security controls at a high level. This discussion is based on real field work assessing the security of these systems. Based on the incidents and events in the past, and the missing gaps in some of the security systems in operation today, the last section of this paper listed some key ingredients to consider when implementing a cyber security system that will be able to defend the threats of tomorrow. By taking a look at the past, present, and future for securing electric power systems, this paper has provided a quick reference guide for those new to this topic.

Lastly, we should address the various groups that share this responsibility. The first group that has the biggest impact on securing our nation’s critical infrastructure is the asset owners and operators of electric power generation, transmission, and distribution systems. Those working for electric utilities have the ultimate responsibility, and now with the NERC CIP standards, are the ones that have to worry about potential fines that can be levied for non-compliance.

The next group is the vendors of SCADA, EMS, and critical cyber devices. The vendor community has a responsibility to manufacture and bring to market components that are secure by default, and continue to upgrade the security of legacy systems. Changes in RFP language, along with the need to comply with NERC CIP is helping drive this.

Another group helping to keep the lights on is the US Federal Government. Both DHS and DOE have seeded money into various initiatives like the National SCADA Test Bed, PCSF, I3P, and various other SBIR-funded programs to raise the awareness of the issues, educate end users, and research and test for vulnerabilities in the SCADA, EMS, and critical cyber device components.

The last group that has helped keep define the future security of the electric sector is the security consulting community. By staying in touch with both the government and vendor communities, and helping write industry standards, this group has become an advocate and partner with asset owners and operators to help establish security programs, policies, procedures that comply with new standards and government regulations. This also involves assessing the current security vulnerabilities, making recommendations to mitigate the risks identified, and assist in upgrading the technology used to physically and electronically isolate and secure SCADA, EMS, and Control System critical cyber systems.

6. References

  http://www.fas.org/irp/offdocs/eo13010.htm

  http://fas.org/irp/offdocs/pdd-63.htm

  http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/warnings/

  https://reports.energy.gov/


  http://www.washingtonpost.com/wp-dyn/content/article/2008/06/05/AR2008060501958.html