Lessons Learned from NERC CIP Applied to the Industrial World

Matt Proctor, Member, *IEEE*, Terry Smith, *Member, IEEE*

***Abstract*— NERC Critical Infrastructure Protection (CIP) Reliability Standards apply to utilities that support the bulk electrical grid in North America and are meant to protect the Grid from cyber-attack. While Industrial facilities are not bound by the regulations outlined in NERC CIP a review of those regulations can help industrial facilities protect their infrastructure from cyber-attack. This paper reviews some of the rules of CIP and how they might help an industrial facility secure their cyber infrastructure. Topics to be covered include: physical security for cyber assets, passwords and password management of cyber assets, event logging of cyber events.**

***Index Terms*—NERC CIP, Security management, Role-Based Access (RBAC), Server Authentication. SYSLOG**

I. Introduction

By its own definition, The North American Electric Reliability Corporation (NERC) is a not-for-profit, international regulatory authority charged with assuring the reliability of the bulk power system in North America. NERC develops, implements, and enforces mandatory Reliability Standards for the bulk power system in accordance with Section 215 of the Federal Power Act. NERC Reliability Standards address the design, planning, and operation of the bulk power system, as well as cyber and physical security.

NERC CIP addresses the security of critical cyber assets or intelligent electronic devices (IEDs), and thus the electrical reliability, in a fourteen separate standards. The pertinent pieces of this standard can be divided into three separate categories: Physical Security, Electronic Security, and Personnel & Procedures.

NERC CIP is meant to prevent an attack that could endanger the bulk electrical system in North America. The loss of the bulk electrical system would have devastating economic impacts to the United States. An attack at an industrial facility wouldn't imperil the bulk electrical system but could cause economic, public safety, or public relations problems for the facility. Since CIP exists to provide cyber-security, it is worth understanding from an industrial prospective to provide cyber-security for industrial facilities. The following sections detail the pertinent parts of NERC CIP.

A. CIP-006 Physical Security of Cyber Systems

NERC CIP-006 addresses the Threat Vector pertaining to physical access. It roughly outlines the methods to control, monitor and log physical access.

B. CIP-002, -003, -005, -007, -009 Electronic Security

1) 002 – Identification of Cyber Assets.
In order to make a critical system secure, its critical components must first be identified. Any equipment that, if compromised, may pose a threat to critical electrical reliability can be classified as a Cyber Asset.

2) 003 – Documentation of Cyber Security Policies.
A key component to any security plan is to ensure that it is well-documented. The personnel must be trained to implement that plan, and the plan should be audited periodically to ensure that it is followed and it is accomplishing its purpose. This section details effective implementation of procedures and the proper documentation.

3) 005– Electronic Security Perimeter.
In order to secure a critical network, all access points must be identified. This section recommends documentation of all devices that include access points, a network diagram including physical layout for example. A continuously updated controls access list, the user permissions database from the RADIUS server, for example, is also recommended.

4) 007–Ports and Services.
The documentation of a secure system should include a comprehensive list of all enabled ports. Maintaining a folder of all settings of all security devices is recommended. Network switches settings, firewall settings, gateway settings, protective relay settings, variable frequency drive (VFD) settings, PLC settings. Any device that has a password should have a configuration or settings file that can be used as a baseline in the event that tampering is suspected.

5) 009–Recovery Plan Specifications.
In the event that a cyber-security event occurs, there must be a plan to remedy the situation. People must be assigned with certain tasks of re-loading firmware and/or settings of equipment. There should be a checklist to ensure that all corrupted equipment has been addressed.

C. CIP-004, -008 Personnel & Procedures

1) 004–Cyber Security Training Program

NERC requires that specific personnel are identified to execute defined cybersecurity tasks. These personnel must be trained at least once per 15 months on all aspects of the plan, including access control, system monitoring and testing, recovery plans, incident reporting procedures and audits.

2) 008 – Incident Reporting & Response Planning

The Incident Response Plan must be tested and rehearsed once per 15 months.

II. Threat Vectors and Threat Actors

Threat Vectors are the means through which attacks are carried out, and Threat Actors are those entities that utilize a Threat Vector, either willfully or ignorantly.

A. Threat Actors

Typical human threat actors can be categorized as disgruntled employees, malicious activists, state-sponsored saboteurs, or members of a crime syndicate. Human threat actors' motivations can range from principled (political goals, social upheaval), to self-interested (profit), to downright ignoble (chaos, bragging rights).

Non-human threat actors consist of bot networks or malfunctioning or improperly configured equipment. Bot networks, originally created by a human threat actor for a specific purpose can lay dormant for extended periods of time and can be triggered into action after a specific event or at random. Malfunctioning or improperly configured equipment can create unintended consequences that have the same result as an intentional attack. For example, malfunctioning equipment may create excessive network data traffic that can appear to be a coordinated denial of service (DoS) attack. It is estimated that 80% of all reported DoS attacks are actually due to malfunctioning equipment (Citation).

B. Threat Vectors

1) Physical

Malicious Threat Actors who have physical access to critical infrastructure clearly pose an imminent danger to electrical or process reliability. Physical access allows actors to take local actions or insert bot networks or take remote actions to other parts of the facility.

2) Cyber System

By NERC definition, a Cyber System contains Cyber Assets "…that if rendered unavailable, degraded, or misused would, with 15 minutes adversely impact [electrical reliability]." Threat vectors for industrial facilities for the cyber system consists of any malicious or erroneous action that would compromise the facilities process. Examples include:

- Probing the systems control or protection networks for weaknesses.
- Changing protective or control settings that would shut down or damage the process at a later time.
- Installation of Bot Networks to damage or shut down the process.
- Direct control of equipment to shut down or damage processes.

3) Personnel & Procedures

Without the proper training and procedural design, the very people who are tasked with protecting electrical reliability can themselves become threat vectors. The information security concept of "social engineering" is a technique that Threat Actors use to manipulate human decision making in order to meet their own malicious goals. Some examples of social engineering include:

- Pretexting, where an elaborate lie might be told in order to trick a person into executing a malicious command.
- Phishing, where a computer user might be tricked into providing classified or confidential information, typically via e-mail.
- Baiting, where an unsuspecting person is tricked by means of curiosity, greed, or even amity to install an infected disc or storage device.

III. NERC CIP and Application to Protective Relays And Control Systems in Industrial Facilities

The first task of the individuals assigned to execute the plans defined by the NERC CIP framework is to perform a risk assessment and identify critical assets. An intelligent electronic devices (IED) in an industrial facility qualifies as a critical asset if it meets one of these criteria:

- The IED is capable of tripping a breaker that would interrupt electrical supply to one or more critical loads.
- The IED is capable of closing a breaker in a manner that would tie together two sources that are out of synchronism.
- The IED is capable of energizing a load at an improper time or in an improper intermittent fashion that may result in excess thermal stress and/or voltage and frequency degradation.
- The IED is capable of initiating a communications signal to another device that will result in an improper breaker operation.
- The IED is capable of transmitting excessive data on a communications network that may prevent that network from performing its critical mission.

Once an IED is determined to be part of a network that has the ability to control critical operations, the analysis of the electronic security perimeter must be expanded to include other components that may interface with the IED.

In the context of an industrial facility's electrical network, this may be:

a) Network switches

b) DCS or SCADA control room equipment used to operate breakers or monitor critical alarms or control critical processes.

c) Load Management/Load Shedding equipment

d) Generator or process programmable logic controls (PLC's)

e) PLC's for black start resources such as fuel gas heaters and other balance of plant operations.

f) Safety Instrumented Systems(SIS) PLC's.

After the assessment of IED's, identify the necessary security features that are available in modern protective relays.

Modern protective relays can help meet these requirements using the following methods:

1) RADIUS Authentication

Remote Authenticaion Dial-In Service (RADIUS) is a method of authorizing user access using a centralized database of users and permissions rights. The same system used for administering key-card access can be accessed by modern protective relays and prevent unauthorized relay manipulation. This can be especially useful to eliminate the most hazardous of threat actors, the disgruntled former employee. A disgruntled employee already knows the weaknesses of the system and the security measures, including the passwords of the cyber assets across the facility. When a central RADIUS database is used to authenticate access to all cyber assets, the disgruntled employee's access can be completely revoked with one action.

When authenticating users to a protective relay or control system, not all users will require the same access. For example, the field personnel may need access to view settings and metering data but not to change settings. Role based access of the device is necessary to ensure that only the correct personnel have access to the correct information. Role based access can be used in conjunction with RADIUS authentication to define the role that the uses has and then the device can only allow the user to access the information available for his role.

2) Alarming Distributed Control System (DCS) or Substation Control And Data Acquisision (SCADA) system

Modern relays can be programmed to interface with a DCS or SCADA system. By virtue of being continually monitored, these systems offer the earliest warning if there is an intrusion into a secure area.

3) Computerized Logging - SYSLOG

Modern relays are capable of maintaining a time-stamped log of events. The relay can instantly publish pertinent data when a relay is physically accessed through the front panel. Access can mean that a user has pressed a pushbutton, jumpered a contact, locally connected to the relay using a computer or attempted to access the relay but was denied. The relay can then publish a time-stamped stream of data that contains all known information including the type of operation, the user credentials, MAC address and IP Address (if applicable). This continuous stream of information can be connected to an off-site server where it is securely stored for security audit purposes.

4) Firmware Management

Firmware manipulation is a threat vector in which a device's electronic DNA is altered to cause the device to operate in a harmful manner. IED's should have the capability to alarm or shut down when improper firmware is detected, and firmware should be written to the device only through the manufacturer's software. This can be accomplished by designing the IED to require an encrypted, SSH file transfer. Thus, malicious firmware from a third party software tool or USB drive would be prevented because only the manufacturer's software contains the SSH encryption key.

Relay firmware updates should be checked periodically, and security-related firmware should be updated as quickly as possible when a security patch becomes available.

IV. Defense in Depth (and How Relays Play a Role)

The strategic concept of Defense in Depth is to devote resources not only to the obvious imperative of securing the perimeter but also to impede the destructive force of an attack if that perimeter is breached. The three areas of Defense in Depth closely mirror the three classifications of threat vectors: physical, technical and procedural.

A. Physical Security Perimeter (PSP)

Arguably, the most important line of defense is physical security. If a bad actor gains physical access to critical equipment, it is evident that the equipment can be shut down or damaged locally. A good Defense in Depth implementation would limit the scope of damage despite a local breach. For example, someone might hack a gate key for entry into a control building. The amount of time that this person has to act should be limited by following the CIP-006 guideline that recommends an alarm for unauthorized access, perhaps by motion sensor. Subsequent breaches by the same bad actor might be prevented by capturing images of the perpetrator using security cameras.

If Defense in Depth can be applied to physical security, with different access keys applied at different control houses within an industrial plant. This would serve to impede the malicious progress of a bad actor who would be forced to pick or hack multiple locks.

Physical access to an IED or Ethernet switch can be impeded by installing relays in locked control cabinets.

B. *Technical Security*

1) *Electronic Secure Perimeter (ESP)*

NERC CIP-005 provides a framework for establishing an Electronic Secure Perimeter (ESP). The intent of an ESP is to identify any equipment that may be capable of communicating beyond the perimeter and take certain precautions to make sure unauthorized communication does not enter or escape the perimeter. Any equipment capable of communicating via a routable protocol should be classified within the ESP. This includes (but is not limited to) equipment that communicates using common industrial communications standards as Modbus TCP/IP, DNP/IP, or IEC61850 MMS. Basically, any device with an Ethernet port should be considered part of the ESP.

It is important to note that even standalone networks, those networks that are not connected to the internet or even broader networks without an internet connection, should be regarded as assets within a ESP. Isolation is not a reliable security plan because malicious code can be implanted from within an isolated network, and isolated networks can be connected to broader networks without authorization. A simple mistake like connecting a cable to the wrong port can create an unwanted connection, or an uninformed employee can intentionally create an unsecure connection with the well-intentioned purpose of increasing productivity. A good Defense in Depth strategy recognizes these threats and limits potential damage in the event that these breaches occur.

2) *Electronic Access Point (EAP)*

NERC-CIP-005 advises that any connection to the ESP from the outside should be managed by an Electronic Access Point (EAP). An EAP's function is to control inbound and outbound data traffic. This includes limiting the type of traffic that can flow on the network and the range of network addresses. For example, if a SCADA control network relies entirely on IEC 61850 messages, the EAP can be programmed to block any traffic that does not have the data structure of a 61850 message. This eliminates the opportunity of malicious code or commands from reaching the target. In the event that a bad actor attempted to make a Telnet connection over the network to issue a simple ASCII command, "PULSE OUT 101" to exploit an IED's proprietary command-line interface, this action would be thwarted.

An EAP should be used to whitelist certain addresses of devices that are authorized to communicate on the network. If a SCADA network is intended to be operated by one single command terminal, the IP address and MAC address of that server should be the only item allowed to broadcast messages into the ESP. The IP addresses of IED's on the network that must publish information for consumption outside of the ESP should be whitelisted for that purpose.

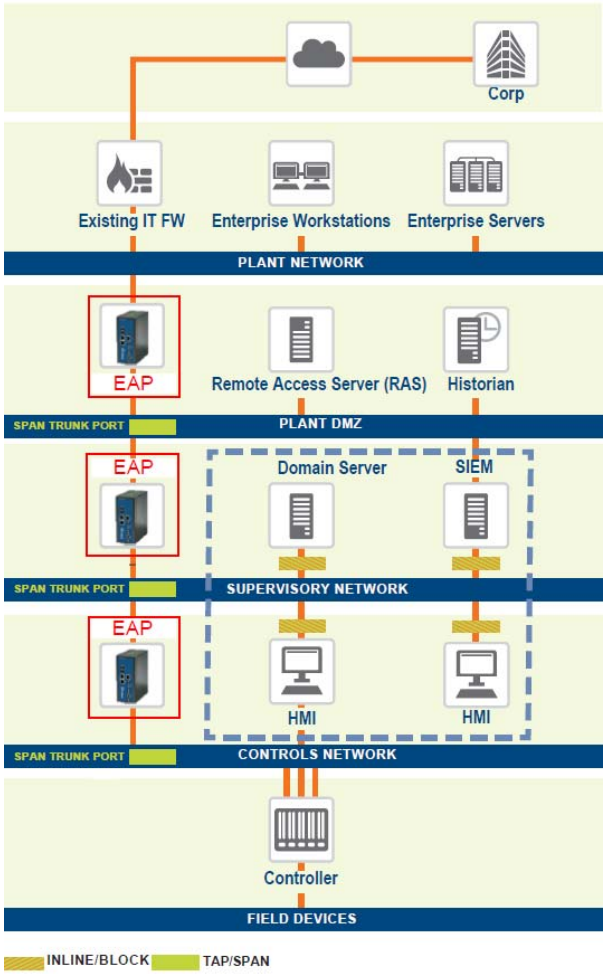

Figure 1: Example deployment of EAPs

NERC requires a method of flagging and reporting suspicious data traffic when it is detected. Many cyber attacks will begin with probing for information on the control system architecture and control system cyber protection. The ability to detect probing attacks and alarm for intrusion allows operators and security personnel to act to secure the system and prevent further attack. Additionally, the cyber system must be secure enough so that a probing attack cannot be applied as a Denial of Service (DoS) attack.

A brute force attack consists of repeatedly trying to guess a password. In theory, an automated computer system would be able to enter enough password attempts to correctly enter the password in a matter of time. NERC-CIP requires that any equipment within the ESP which requires a password must be capable of notifying operations personnel in such an event. This can be accomplished by alarming a DCS system or by periodic monitoring of a syslog security system.

Access lockout can be used to slow automated brute force attacks. After an unsuccessful number of password attempts, access lockout requires a user-selectable lockout duration before subsequent password attempts are allowed. This would allow the system sufficient time to notify operations personnel to take action.

C. Personnel Training and Operations Response

Although a good Defense in Depth strategy involves restricted physical access and cyber access including logging and alarming, these measures are largely useless without properly trained personnel to implement these strategies. Cyber security is after all a human endeavor.

1) Identification of Roles

Especially in larger organizations with many employees and many specialized technical capabilities and functions, it is imperative to ensure that role-based access is granted only to those persons who are trained to perform that task.

The data available in the IEDs can be separated into two different uses: operational data and non-operational data. Operational data represents the real-time status, performance, and loading of the power system or control system. This is fundamental information used by the operators to monitor and control the power system or process. Non-operational data is data which the primary user is someone other than the system operators such as engineering or maintenance. Securing the IEDs while still making non-operational data available remotely can be a challenge. Enterprise management software can allow devices to create secure tunnels through the secured networks and send the non-operational data to a secure server. The data can then be served to users from the secure server. This type of data collection not only makes it easier to obtain non-operational data but it can also be used to secure the system by alarming when a settings change is noticed from a baseline or when the IEDs don't have the baseline firmware.

In addition to dividing the operations tasks through RBAC, NERC recommends designation of a Security Incident Response Team. Just like an office building likely has a floor marshal who is designated to take appropriate action in the event of a fire or other safety threat, an industrial plant should have a team responsible for responding to a cyber threat. There should be a pre-determined response for any conceivable condition. This can range from routine management of access credentials or response to security exploit bulletins to more climacteric tasks like implementation of a catastrophe response plan.

V. Specific Examples of Security Problems and How to Address them

A. Stuxnet-2009 [1]

This well-publicized attack targeted Iranian uranium enrichment centrifuges. It is the first example of a cyber-attack creating physical damage to equipment beyond the cyber world. It is also a good example of an attack against a network that was supposedly isolated. The threat actors in this case are widely suspected to be state-sponsored actors.

The attack took advantages of many different threat vectors. Engineering contractors known to be configuring the centrifuge motor PLC's for the Iranian government were unwittingly used to spread the malware via infected USB storage devices. The code was very specifically designed to take advantage of a known exploit in the PLC software that required use of a default password to establish connections with the PLC.

Because this attack is particularly intricate, there is no way of knowing for certain that is could have been stopped. But some of the tools that could have made this attack more difficult are:

- Better training and reporting procedures could have prevented the attack as it is known that the contractors suspected that the software was compromised. They posted their suspicions on an online help forum prior to the discovery of Stuxnet and noted that they did not have a problem with machines where the software had been installed from a CD as opposed to the USB install.
- More robust password management at the hardware level.
- Stronger IT restrictions on installation of software on behalf of the contractors.

B. German Steel Mill Hack - 2014[2]

In another example of a cyber attack creating physical damage, a German steel mill was targeted by a malicious actor with unpublished motives. This actor gained access to the company's corporate network using spear phishing e-mails, e-mails that look like official business but in reality are carefully crafted gimmicks that carry attachments infected with malware. It is suspected that the bad actor performed internal reconnaissance using tools like key loggers and network scanners before finding a way into the mill control network. Once mill control network access was obtained, the bad actor had the savvy to manipulate the furnace controls and operated it in an intentionally damaging way.

This attack may have been prevented using the following methods:

- Better employee training to recognize phishing.
- Use of EAP technology that can segment network traffic and/or alarm after detecting malicious data once the key logger or network scanning was implemented.

C. Cyber Attack on Ukraine Power Grid-2015

In 2015, a Ukrainian utility company experienced an attack that resulted in outages at seven 100kV and twenty-three 35kV substations, affecting over 225,000 people for about three hours. This instance of cyber-intrusion details another intricate malicious operation likely carried out by a state-sponsored actor. Much like the German steel mill attack, the operation involved reconnaissance, network infiltration

followed by data-gathering and finally malicious use of the control network to open breakers. Adding insult to injury once the attack concluded, the serial-to-Ethernet converters were effectively destroyed with a malicious firmware. This removed the possibility of restoring power from the central control room. Instead, it was necessary to dispatch crews to each of the thirty affected substations in order to close the breakers and restore power.

Using the framework of NERC-CIP, this attack could have been impeded by:

- Utilizing hardware that disallows a firmware upgrade through a network connection without an encrypted connection.
- Periodic checking of a syslog system that would have recorded the malicious traffic during the internal reconnaissance phase.
- Applying a RBAC access system that requires multi-factor authentication prior to executing a breaker open command in the IED's.

VI. Conclusion

Although the technology we use to make our electrical systems more reliable can also be used counter to its purpose, it is important to avoid the temptation to discount the value of this technology altogether. Automation helps us operate electrical systems smarter and more efficiently. Automation helps restore outages more quickly to minimize downtime.

Electrical control systems should be designed and programmed and managed with attacks in mind. In the event of an attack, a good system should have the ability to quickly eliminate the threat and revert to a more secure method of operation, perhaps in a mode that temporarily sacrifices the benefits of that automation.

NERC places a great onus on the "Responsible Entity". It is the "Responsible Entity's" burden to understand the hardware and communications network, to classify the equipment as critical, to install and configure the necessary equipment, to continually evaluate the efficacy of the system, to document and report any potential breaches and take proper corrective action. While it may be a tremendous burden, the cost of securing the cyber assets must be weighed against the risk and potential cost of a malicious attack. In instances where cyber assets have become an indispensable part of plant operations and the risk of becoming a victim of a malicious attack outweighs the cost of implementing a security plan, voluntarily adhering to at least some of the NERC-CIP mandates can make economic sense.

References

Basic format for books:

[1] K. Zetter. (2014, Nov.). An Unprecedented Look at Stuxnet, The World's First Digital Weapon. *Wired*. [Online]. Available: https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/

[2] R. Lee, M. Assante, T. Conway. (2014, Dec.). ICS CP/PE (Cyber-to-Physical or Process Effects – German Steel Mill Cyber Attack). [Online]. Available: https://ics.sans.org/media/ICS-CPPE-case-Study-2-German-Steelworks_Facility.pdf

[3] R. Lee, M. Assante, T. Conway. (2014, Dec.). Analysis of the Cyber Attack on the Ukrainian Power Grid. [Online]. Available: https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf

[4] NERC Critical Infrastructure Protection http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx

Matt Proctor is currently a Technical Application Engineer at GE Multilin and has been with GE Multilin for over 7 years. Matt earned Bachelor of Science in electrical engineering from Louisiana State University in Baton Rouge, LA in 2001 and an MBA from LSU in 2005. He has been working in the electrical power field in various capacities since 1997. He specializes in power system studies and protection and control relay applications.

Terrence Smith is the Commercial Application Director for the GE Grid Automation North American Commercial team. In this role, he leads the team of technical application engineers supporting the Protection and Control, Substation Automation, and Monitoring and Diagnostics portfolio. He joined GE in 2008 supporting the Grid Automation Protection and Control Portfolio. Prior to joining GE, Terrence has been with the Tennessee Valley Authority as a Principal Engineer and MESA Associates as Program Manager. He received his Bachelor of Science in Engineering majoring in Electrical Engineering from the University of Tennessee at Chattanooga in 1993 and is a professional Engineer registered in the state of Tennessee.