21, rue d'Artois, F-75008 PARIS
http : //www.cigre.org

CIGRE US National Committee
2016 Grid of the Future Symposium

Applying NERC CIP Standards to Power Distribution Utility Control Centers to Enhance Cybersecurity within a SMART and Automated Environment

J.M COLE
Sargent & Lundy, LLC
USA

N. WALLACE
Ampirical Solutions, LLC
USA

SUMMARY

The recent cyber-attack against a Ukrainian Power Distribution Utility on December 23, 2015 has raised concerns for many utilities in the U.S. and throughout the world. Some transmission and distribution utilities are still unaware of the specifics of this attack and are amazed that it affected only the distribution supply. What are utilities doing within the U.S. and Canada to ensure resiliency against such an attack? The North American Electric Corporation (NERC) created its Critical Infrastructure Protection (CIP) Standards under the jurisdiction of the Federal Energy Regulatory Commission (FERC) in order to prevent possible cyber attacks to the Bulk Electric System (BES). NERC's primary mission enforces its CIP Standards upon generation and transmission utilities regulating them to harden their critical cyber assets (CCAs) that connect to a routable Internet Protocol (IP) against potential hacking vulnerabilities [1]. According to NERC, distribution power voltages ranging from 69kV and below are considered to be "very low" or have "no impact" on the BES ranging at voltages well above 100kV.

The most recent NERC CIP Version 5 (V5) standards currently in affect do not include regulations for power distribution utilities. With no CIP standards or governing entities controlling the distribution utilities against cyber-attacks today, the greatest fear is that several power distribution utilities in the U.S. and Canada could be less secure and more vulnerable than Ukraine on December 23, 2015. Although power distribution grids present very low or no risk to the BES, if threatened with a major attack, cities could be affected by blackouts which would be particularly costly if not fatal.

With the NERC CIP V5 regulatory deadline of July 1, 2016 for transmission utilities behind us, how many transmission utilities were compliant by the deadline? How many transmission utilities in the U.S. and Canada remain vulnerable similar to distribution utilities? How will distribution utilities defend themselves in preparation and protection from adversaries aiming to disrupt their power grid? Distribution utilities at least need a guide or method for protecting CCAs within their control centers. The purpose of this paper is to raise awareness among the power distribution utilities by applying some of the NERC CIP standards to distribution control centers to ensure resiliency through enhancing cybersecurity and eliminating possible vulnerabilities. Though there are other cybersecurity frameworks and recommended best practices (e.g. NIST, CIGRE & IEEE), NERC CIP represents the only set of standards federally required in the U.S. and Canada and is therefore the focus of this paper.

KEYWORDS

Communications system security, Communication networks, IP networks, Power distribution, SMART grid, SCADA, Automation, Compliance

joseph.m.cole@sargentlundy.com

1. INTRODUCTION

Over fifteen years ago, cyber-crimes were minor and reduced to stealing identities, credit card fraud, long distance calling or corrupting personal computer (PC) hard drives with viruses and malware. These crimes have intensified over the years to attacking public infrastructures such as banks, businesses, government, and other entities including utilities. With the vast up rise in cyber-crimes, the future points to more advanced, creative and lethal cyber-attacks. The cyber threat to our nations power distribution utilities is very real and its not a matter of "if" it will happen but a matter of "when" it will occur? The Ukraine event should be a wakeup call and lessons learned to all utilities, specifically distribution utilities.

Recently, the Federal Bureau of Investigation (FBI) and Department of Homeland Security (DHS) submitted a warning to all U.S. power utilities with 12 briefings informing them of a potential cyber-attack to the electric grid. These briefings discussed some recent cyber-attacks including the Ukraine event with the methods used by the hackers. They proposed possible tactics to be used for limiting risks while improving cyber security [2]. For utilities to do nothing towards enhancing their cyber security is seen by the public to be both risky and irresponsible. As the attackers continue to evolve, NERC tightens its belt by improving its regulatory CIP standards in hopes of preventing a future attack to the BES, which currently provides no aid for distribution utilities. This paper aims to help distribution utilities apply some of the appropriate CIP standards to their control centers for cyber resiliency while in an automated, SMART Grid environment.

The Ukraine event was a well-planned and successful attack carried out by cyber criminals that remotely gained full remote access control to Ukraine's control centers' critical network and power operations. The attack involved opening all supply breakers at 30 substations ranging from 35kV to 110kV leaving 225,000 customers without power for up to 6 hours. The infectious and undetected intrusion began more than 6 months prior to the attack by spear phishing emails that ultimately loaded the vicious BlackEnergy 3 malware. Data logger and keystroke logging techniques were implemented to capture users' credentials and passwords to access virtual private networks (VPNs) and other enterprise networks [3]. This allowed the adversaries full access to the utility's supervisory control and data acquisition (SCADA) and human machine interface (HMI) systems. During the attack, hackers created a diversion by implementing a telephone denial-of-service attack on Ukarine's telephone call center servers. The diversion was successful by keeping the utility's staff preoccupied and unaware of the main network cyber intrusion. This also prevented customers affected by the power outages from reaching the call center to notify utility personnel of the outages. These cyber criminals successfully shut down the uninterrupted power supply (UPS) systems providing power to the control center equipment. They gained full access and control to the power operators' workstations ultimately controlling parts of Ukraine's power grid. When the damage was done, the adversaries implemented the KillDisk sequence erasing all data from workstations, servers and network devices, leaving them inoperable [3]. "The incident in Ukraine still remains the first possible instance of a blackout caused by a malicious network intrusion." [3] Ukraine was left with sending substation operators to de-energized stations in order to manually operate breakers for power restoration that were previously tripped by hackers.

1.1. Other Threats and Concerns

A recent cyber-attack that hit a hospital in February 2016 at the "Hollywood Presbyterian Medical Center demonstrated criminal hackers' willingness to put lives at risk for a payday. The attack method, known as ransomeware, locked employees out of the hospital's system in an attempt to shut down the hospital. While the center's chief executive said patient care was not compromised, the hackers crippled computer systems, forcing employees to use pen and paper for record-keeping." [4] Another incident at the Lansing's Board of Water & Light took a week to recoup from a ransomware cyber-attack that struck its business critical and enterprise systems. "The successful phishing attack on its corporate systems, which was first noticed on April 25, forced the utility to keep systems,

including phone servers, locked down." [5] Ransomware encrypts all data in its path, with infections starting with the first PC spreading to the entire network and infiltrating the critical enterprise systems.

Another unbelievable and unfortunate attack that happened in May 2015 was against our own Federal Government's computer network with a data breach where hackers gained access to nearly 22 million records of government background checks. The cyber criminals gained access to sensitive information for personnel files including background checks processed over the last 15 years with data ranging from fingerprinting, social security numbers, health records, education transcripts, employment history, financial data and other personal information. Just one month prior, personnel data was stolen by hackers on 4.2 million federal government employees, which included sensitive data on intelligence and military personnel [6]. The Obama Administration recently asked congress to approve another $19 billion in increased government spending for cyber security protection and equipment improvements [7]. Cybersecurity protection will continue to be of great concern for the U.S. since over the next 3 years or by 2020, it is estimated that nearly 20 billion new devices will be connected to an Ethernet routable, IP network.

2. DISTRIBUTION CONTROL CENTERS

A distribution utility's control center is the heart and soul for operating and controlling their power grid. A Smart Distribution Control Center (SDCC) is characterized by the functions and operational capabilities of the center and is comprised of an increased reliance on data acquisition, software, and automation. The center will permit the control and automatic management of: demand response, peak demands, loads, power quality, distributed generation, and distributed storage [8]. Derived from NIST's *Guidelines for Smart Grid Cybersecurity*, Figure 1 shows the operational function blocks for a SDCC.

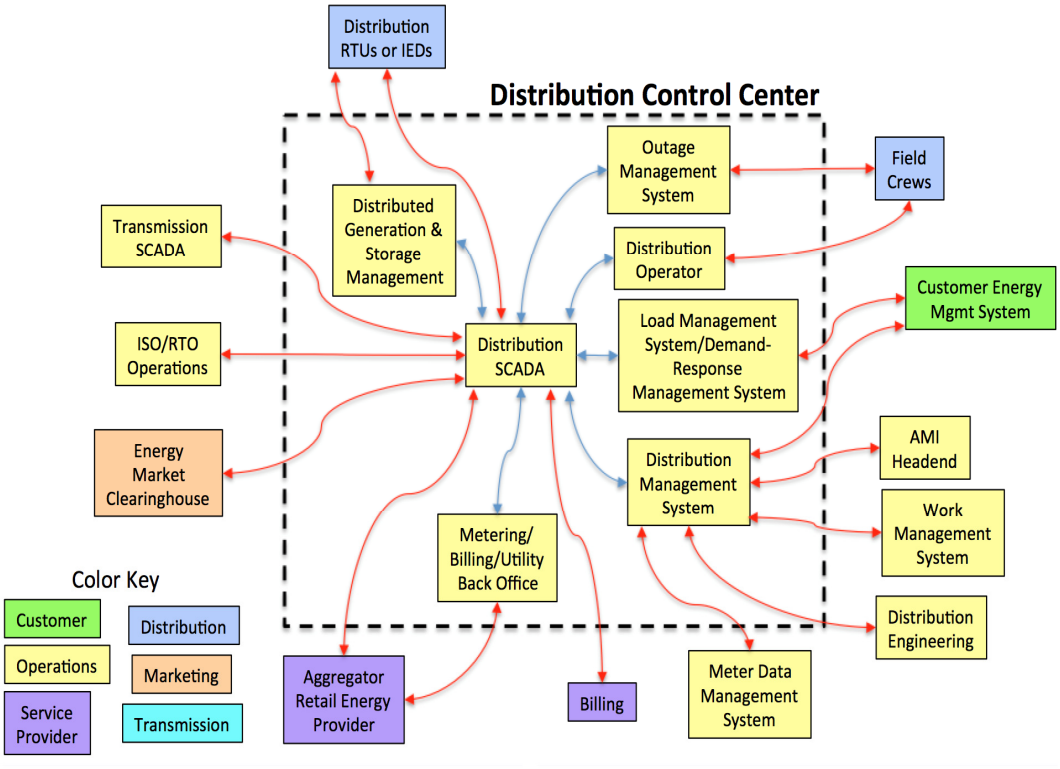

Figure 1: ***Smart Distribution Control Center, Smart Grid Logical Reference Model*** **[8]**

The typical operations of an SDCC are shown enclosed in the dashed box of Figure 1. Links connecting each function block depicts the physical flow of data and are labeled as logical links that

occur within the center's electronic perimeter. In order to effectively reduce the associated risk and therefore to help ensure the safety and reliability of the SDCC environment some level of cyber links, shown in red identify potential communication paths with entities or assets physically outside the control center, while links shown in blue represent communications between functions where protection and controls (P&C) should be implemented. The CIP standards described in the next session should be considered by distribution utilities even if the current regulatory and jurisdictional landscape does not directly require the implementation.

3. NERC CIP STANDARDS

The major regulatory push to apply cyber security measures in the electric utility industry within the U.S. and Canada is the result of the NERC CIP standards. Under the order of FERC, asset owners are required to adhere to each standard based on applicability and regulatory jurisdiction. The NERC CIP standards only apply to assets and systems that relate to the BES. In some cases, the same technologies that permit the implementation of NERC CIP standards in BES Cyber Systems can be used to facilitate the same standards in a SDCC. In instances where entities are also responsible for assets across generation and transmission systems, it is advised that the resources and knowledge applying the CIP standards in these systems are fully leveraged when also applying them to their distribution level.

For distribution providers, NERC CIP applicability is based on a threshold value of 300 MW as it relates to automatic and non-human initiated load shedding capabilities. This distinction, though it helps draw a line, can be viewed as irrelevant from the cyber perspective. For distribution control centers whose substations move a net power greater than 300 MW can be viewed as applicable regardless of automatic load shedding capabilities. In the case of the Ukraine event, adversaries were able to de-energize multiple stations while locking out the operators' ability to remotely recover. Table 1, shows the typical NERC CIP standards that can be applied to distribution utility control centers [11]. Although recommended for distribution utilities and further research, some CIP standards' and their applications were not included within the scope of this paper.

Table 1: ***NERC CIP Standards to be Applied to Distribution Utility Control Centers*** **[11]**

NERC CIP STANDARDS	TITLE/DESCRIPTION	RECOMMENDED FOR DISTRIBUTION UTILITIES
CIP-002	*BES Cyber System Categorization*	Yes (not included in the scope of this paper)
CIP-003	*Security Management Controls*	Yes (not included in the scope of this paper)
CIP-004	*Personnel & Training*	Yes (preparation & prevention)
CIP-005	*Electronic Security Perimeter(s)*	Yes (intrusion detection & prevention)
CIP-006	*Physical Security of BES Cyber Systems*	Yes (restricted access)
CIP-007	*System Security Management*	Yes (logging, patch management)
CIP-008	*Incident Reporting and Response Planning*	Yes (awareness and learning)
CIP-009	*Recovery Plans for BES Cyber Systems*	Yes (recovering from an incident)
CIP-010	*Configuration Change Management and Vulnerability Assessments*	Yes (decreases attack surface)
CIP-011	*Information Protection*	Yes (appropriate handling of sensitive data)
CIP-014	*Physical Security*	Yes (not included in the scope of this paper)

3.1. CIP-004-6 Personnel & Training

The CIP-004 standard is recommended for all utilities including power distribution utilities. The biggest tool and perhaps the weakest link of any utility's security program is their personnel. To help cut-down on insider threats, Version 6 of CIP-004 now requires all personnel (employees and contractors) to undergo a seven year background check prior to gaining access to restricted areas. Once granted, a review of all accounts and privileges must be carried out periodically. In instances where the removal or change of an account is required, a process must be in place initiating the

deletion or revision of an individual's permissions. Additionally, upon a change in an individual's permissions, all shared accounts are required to be updated within 30 calendar days. For large control centers with abundant personnel changes, this can become a cumbersome task to perform manually. Similarly, for centers with a relatively small number of employees, effectively updating and changing all permissions can be challenging if the updates are performed only a few times a year, resulting in items being neglected. There are several technologies on the market that permit the automatic updating and management of users' credentials across multiple software packages, services and devices (e.g. Siemens Crossbow). Utilities should consult their information technology (IT) departments to help determine the feasibility of such systems or seek outside assistance where needed. Lastly, it is recommended that asset owners start to ask vendors for applications and devices that support authentication and authorization capabilities.

After all accounts are verified and managed properly, authorized personnel are required to undergo periodic training. Ideally, this training helps individuals learn about the latest threats, trends, and security measures while providing a refresher on company security policies and procedures. Often times this type of training can be overshadowed by basic security training objectives related to password management and avoiding phishing attempts. A list of training content specifically called out in this CIP standard include: (a) cyber security policies; (b) physical access controls; (c) electronic access controls; (d) handling of information; (e) incident identification and notification; (f) response and recovery; (g) cyber security risks. This training is required for all individuals with granted access and must be carried out at least once every 15 months [7]. When possible, it is recommended that training be carried out in the context of the environment the personnel are working.

3.2. CIP-005-5 Electronic Security Perimeter(s)

It is recommended that distribution utilities identify and designate all cyber assets (CAs) connected to a network via a routable protocol within an electronic security perimeter (ESP). All external routable connectivity (ERC) must pass through an identified electronic access point (EAP). CIP-005 requires all inbound and outbound traffic to have access permissions, and the ability to detect known or suspected malicious communications. Additionally, for all Interactive Remote Access (IRA) sessions, communication paths exiting the ESP must utilize encryption and multi-factor authentication. As depicted in Figure 1, a SDCC can be comprised of multiple function blocks with design specifications requiring logical communication links with entities and functions outside a center's physical security perimeter (PSP). The red links in figure 1, mark those communication paths where data travels through the center's ESP. These paths should be reduced to the least number of EAPs. For instances where only one-way communication is needed entities could consider data-diode technology (e.g. Owl Computing Technologies).

Firewalls should be installed at each EAP equipped with default deny-all policies. Each application can be added later to the firewall's permissible communications creating what's known as white listing of trusted applications and services. Sophisticated techniques in network security monitoring (NSM) should be deployed at each EAP as a means for intrusion detection and are capable of detecting malicious activity even in a firewall's white listed application by performing deep packet inspection. With some firewalls susceptible to their own set of vulnerabilities and configuration errors, NSM installations can help detect and alert upon a number of anomalies and cyber events. For an extra layer of security, control center engineers can also consider placing NSM tools strategically within an ESP to detect malicious activity spreading between internal applications and devices. This type of malicious lateral movement was demonstrated by both the infamous Stuxnet virus [10] and the Ukraine attacks [3]. Distribution providers are encouraged to take a risk-based approach when determining which control center assets should be included inside the ESP and therefore protected. For example, if a declared low impact asset is on the same logical network as a critical device performing one of the operational functions shown in Figure 1, then that low impact asset should be treated with the same security precautions as the critical device. Such an approach decreases the likelihood malicious software will be able to move laterally within the control center.

3.3. CIP-006-6 Physical Security

Distribution utilities should implement clear and defined operational controls for a physical security program to be effective in restricting access to a physical security perimeter (PSP). Each control mechanism should consider how the technology is going to be supported and managed by the control center's engineers and network administrators. For instance, upon adding or revoking access, the control mechanisms should be automatically updated to reflect these changes. Additionally, an alarm or alert has to be issued within 15 minutes of detecting unauthorized access. Exact implementation of this requirement depends on the capability of the installed access control technology. An example of a future control access mechanism may include systems capable of using motion sensors to allow intelligent access control software to count the number of people in the control center and compare it against the number of badged-in and badged-out personnel. If the number of detected personnel exceeds the difference in badged-in versus badged-out, an alarm triggers. For accountability reasons, all access entries require instant documentation. This information is invaluable when determining who's in the control center during or leading up to a misoperation or cyber event (e.g. Cisco, Siemens and Honeywell Security). Where feasible these systems should not be directly connected to the control center's operational network as this may provide a vulnerable situation allowing an attacker to gain access to restricted applications. Lastly, all security control mechanisms should be tested at determined intervals (not to exceed 24 months) and after making any hardware or software changes.

3.4. CIP-007-6 System Security Management

For large distribution utility control centers with multiple primary and back-up cyber systems, carrying out basic security policies can be a daunting task. All cyber assets that support or facilitate the operational objectives of the control room should be taken into consideration when implementing protective measures. For instance, during the Ukraine event the attackers were able to target the applications managing the center's UPS, which ultimately disabled the control room's power. Though this tactic may present itself as being sophisticated, a majority of the UPSs on the market are configured via a web interface and are typically set with default login credentials. Based on the level of awareness and the perspective of a control center's security team, the UPS and similar supporting systems may not be classified with the same security level as an operators' login interface. It is therefore advised that utilities take into consideration the full range of cyber contingencies when determining in and out of scope assets.

After identifying each applicable cyber asset, a number of protective cyber policy measures can then be implemented universally across all assets within the ESP. Two proactive measures include the management of ports and patches. A new installation of the Microsoft Windows Operating System (OS) will generally have between 5 and 10 logical network ports open. After installing the necessary applications (NTP, HMI, OPC, SCADA software, etc.) this number can climb to over 20 and may include open ports that are not required. It is recommended to close all unused services and opened ports. Additionally, the standard requires that a process for tracking, evaluating, and installing cyber security patches be in place. This tracking and installation process should examine both operating system patches and application specific patches. Prior to installing a patch in a live operational environment, it should be tested by a rigorous evaluation process in order to ensure the patch does not adversely impact the operations. This process can be carried out in a sandbox or test bed environment that replicates the OS and applications running on all production machines.

In addition to having a port and patch management process in place, the standard requires active measures to deter, detect, and prevent malicious code. Each one of these abilities can easily encompass a large number of technologies and in the same way all protective relays are not created equal, each type of protective cyber system is also not created equal. Detection of malicious code can encompass the following cyber protection systems: anti-virus software, firewalls, and host or network based intrusion detection/prevention systems (IDS/IPS). When selecting security approaches or

implementations, the following key points should be examined by the security team and design engineers. Selected security technologies should:

- Offer value that is greater than the purchase cost
- Provide real-time or near real-time detection, alerting and logging of cyber events
- Offer a secure means to receive updates if it utilizes a signature based detection approach
- Perform testing in a sandbox environment that reflects the applications and hardware of the production environment prior to live installation
- Not adversely impact the operational environment of the control center
- Monitor all ingress and egress communication of the center's ESP(s)
- Be vendor supported and easily managed by trained personnel
- Allow for easily extractible and forensically sound information

Some examples of vendors who provide various forms of malicious code detection are Tripwire, Cisco, and Fireeye. For the purpose of auditing and for performing forensic analysis, it is vital that all events are logged and stored for an accepted period of time. The standard specifically identifies the following items as events that should be logged: (a) successful logins, (b) failed access and failed login attempts, and (c) detecting malicious code. The logging system should be engineered in such a way that if the logging functionality fails, a notice or alert is sent to the administrative personnel. Logs should be sampled periodically even though no alerts are triggered. Additionally, where feasible, the number of failed login attempts should be limited and a lock out mechanism implemented after a declared number of login attempts. This approach helps prevent any automated brute forcing attempts.

3.5. CIP-008-5 Incident Reporting and Response Planning

NERC created the Electricity Information Sharing and Analysis Center (E-ISAC) portal as an information sharing tool for all utilities including distribution utilities. The E-ISAC portal shared the news of the Ukraine event shortly after it took place. "Institute employees joined with other members of the Electricity Information Sharing and Analysis Center in assessing lessons from the Ukraine incident. Together they issued a report consolidating the open source information to correct media reports, clarify important details surrounding the attack and recommend ways to guard against similar attacks. It is one of several on-going collaborations to grasp and share lessons still being learned". [7] The process to review and report incidents to E-ISAC are not to exceed one hour and can be a preliminary notice. The incident reporting exercise is a must for all utilities. Distribution utilities should implement planning procedures and training for proper response reporting.

3.6. CIP-009-6 Recovery Plans

Similar to storm restoration plans, distribution utilities should have an established cyber recovery plan to efficiently recover from a cyber event. During the Ukraine event, a wiper virus was installed and executed within the control center's ESP in an attempt to completely erase the hard drives of various critical assets while impeding the recovery efforts as long as possible. This tactic to hack the center's UPS systems by disabling power laments the fact that security teams need to consider the full range of different possibilities and craft a recovery plan for each contingency accordingly. Proper back-ups and secure storage allow operators to quickly bring the system and assets back online. Additionally, key personnel should be appointed and details regarding the nature of their responsibility should be documented. These recovery plans ought to be periodically tested and updated based on conclusions of the test or as a result of an actual cyber event.

3.7. CIP-010-2 Configuration Change Management and Vulnerability Assessments

It is recommended for distribution utilities to create a baseline configuration list of all the assets defined within an established control center's ESP, consisting of: (a) operating systems/firmware, (b) commercial and/or open-source software, (c) custom software, (d) logical accessible network ports, and (e) installed security patches. Using this list, an internal or external team can compare the baseline list against a list of known vulnerabilities and then can take the appropriate action to mitigate any potential risk posed to the center's operational environment. For control center's with multiple EAPs, the baseline configuration should be periodically monitored for newly announced vulnerabilities. Vulnerabilities with a high criticality score should be examined first and should be considered in the context of the center's operational objectives. By leveraging this impact or risk-based approach, mitigation strategies can be prioritized resulting in minimal operational downtime whenever a patch or hardware change requires mitigating vulnerability. These changes should be tested and verified prior to installation into the operational environment. Once a fix has been issued, the baseline can be updated with the new configuration where the monitoring process continues. In cases where a network exploitable vulnerability has been identified and a direct fix cannot be applied, a signature should be added to an IDS/IPS that monitors the device's communications.

3.8. CIP-011-2 Information Protection

In addition to actively protecting the control center via measures like firewalls, intrusion detection, and encryption, asset owners should also strive to protect the information related to the design and procedures that outline how the control center is operated. By restricting and tracking who has access to this sensitive information, the likelihood of it ending up in the wrong hands substantially decreases. Additionally, as assets are taken out of service the information digitally stored within those assets may also contain sensitive and restricted information. All sensitive information should be stored in a separate and secure location with access restrictions implemented. The information protection requirements apply to both digital and hard copies with appropriate methods for secure handling including storage, transfer and use. Appropriate steps must be in place for overwriting, purging, degaussing and destroying sensitive data that discusses the following but not limited to: cyber asset identification, systems/software/firmware lists, ESP, PSP, security training, security management, policies & procedures, incident reporting, recover plans, etc. It is highly recommended that distribution utilities enforce the necessary actions in order to prevent unauthorized retrieval of cyber sensitive data.

4. CONCLUSION

Though not required for distribution utilities, the NERC CIP standards if strategically implemented, can enhance a system's cybersecurity posture and offer a better chance for surviving future cyber threats. While there are other frameworks and best practices, the NERC CIP standards are the only federally required cybersecurity measurers currently in the US and Canada and provide a solid foundation for asset owners who may already have experience with implementing the standards. This paper recommended key CIP standards to use for power distribution utilities within an automated, SMART Grid environment in order to ensure cyber resiliency. Specifics of some CIP standards for cybersecurity enhancements were applied to distribution utility control centers. Other security techniques were recommended for protecting the ESP located within the SDCC. Implementing an IDS/IPS within the SDCC/ESP is essential for detecting malicious code and cyber intrusions. Updating firmware and software patches on a regular basis is crucial.

Another big incentive in cybersecurity improvement is training and preparing utility personnel for an enormous cultural change. Recovery plans and procedures are a necessity in order to quickly recover from a direct cyber intrusion attack. Proper use of sensitive data is essential in preventing

unauthorized access and retrieval. Additionally, this paper discussed the importance of sharing cyber incidents by informing neighbouring utilities. Remaining abreast of the latest threats is equally important as performing the actual cybersecurity upgrades. The Ukraine attack was an awful and scary experience but it does provide immense lessons for other utilities that are prepping for this event. Utilities performing present and future security enhancements will continue learning from the Ukraine incident for years to come.

BIBLIOGRAPHY

[1] J. Cole. "Challenges of implementing substation hardware upgrades for NERC CIP version 5 compliance to enhance cybersecurity, "in 210 IEEE, Power Engineering Society Transmission & Distribution Conference, pp 1-5.

[2] B. Gertz, "FBI warns of cyber threat to electric grid," April 8, 2016. [Online]. Available: http://freebeacon.com/author/bill-gertz/.

[3] R. Lee, M Assante, and T. Conway, "Analysis of the cyber attack on the Ukrainian power grid," SANS ICS, E-ISAC. [Online]. Available: http://www.eisac.com/.

[4] R. Gupta, "These types of hackers are driving cyber attacks now". March 21, 2016. [Online]. Available: http://www.fortune.com/tag/cybersecurity/.

[5] B. Lundin, "Just an incident: Michigan utility downplays cyber attack," May 4, 2016. [Online]. Available: http://www.smartgridnews.com/.

[6] E. Nakashima, "Hacks of OPM databases compromised 22.1 million people, Federal Authorities Say," July 9, 2015. [Online]. Available: https://www.washingtonpost.com/news/federal-eye/wp/2015/07/09/hack-of-security-clearance-system-affected-21-5-million-people-federal-authorities-say/.

[7] Rueters, "Obama budget proposal includes $19 billion for cybersecurity, " February 9, 2016. [Online]. Available: http://www.fortune.com/2016/02/09/obama-budget-cybersecurity/.

[8] NIST "Guidelines for Smart Grid Cyber Security v1.0," 2010. [Online]. http://www.nist.gov/smartgrid/upload/nistir-7628_total.pdf

[9] US Dept. of Homeland Security, "Recommended practice: Improving industrial control systems cybersecurity with defense-in-depth strategies," 2009.

[10] Nicolas Falliere, Liam O Murchu, and Eric Chien. W32. Stuxnet Dossier. Symantec, version 1.3 edition, November 2010.

[11] NERC CIP Standards. [Online]. Available: http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx/.