IMPLICATIONS OF THE 2015 AND 2016 UKRAINIAN ELECTRIC GRID CYBER ATTACKS TO NUCLEAR POWER PLANTS

Joseph Weiss, PE, CISM, CRISC
Applied Control Solutions, LLC
10029 Oakleaf Place Cupertino, CA 95014
joe.weiss@realtimeacs.com

ABSTRACT

Nuclear plants can be vulnerable from electric grid cyber attacks. In December 2015 and December 2016, cyber attackers attacked the Ukrainian electric grid and "turned off the lights" by opening substation protective relays. The 2015 cyber attacks targeted electric distribution systems and the 2016 cyber attacks targeted electric transmission systems. In order to accomplish the attacks, the cyber attackers compromised field control system devices to inject malware and then open protective relays in substations. There are some very significant implications to nuclear plant operations from hacking the substations and switchyard breakers that serve nuclear plants. The nuclear plant operational concerns are compromising protective relays to prevent relay protection that would result in damage to large electric equipment; spurious actuation of protective relays causing loss-of-offsite power (LOOP) conditions; and the closing and then reopening of protective relays out-of-phase with the grid causing the Aurora vulnerability damaging generators, Alternating Current (AC) motors, and transformers. All of these protective relay conditions have already occurred in actual or test conditions. The common thread to these scenarios are that switchyard and substation protective relays are out-of-scope of existing nuclear cyber security regulations yet, when compromised, have demonstrated impacts to nuclear plant operations and challenged safety systems. There is one other issue about an attack originating from a protective relay. That is, it would be irrelevant whether the nuclear plant system that would be impacted would have analog or digital instrumentation and control (I&C) systems because the impact is upstream of the I&C.

Key Words: Cybersecurity, Aurora vulnerability, Protective relays

1 INTRODUCTION

The purpose of this paper is to provide an understanding of how cyber attacks of the electric grid can impact the operations of nuclear power plants including challenges to safety systems. The author is a nuclear control system engineer that supported the U.S. Nuclear Regulatory Commission in the development of Regulatory Guide 5.71 as well as the U.S. Department of Defense on the Aurora hardware vulnerability. The Ukraine suffered, and continues to suffer, from on-going cyber attacks in many sectors including rail, mining, airports, finance, and electricity. This paper will focus on the cyber attacks against the electric sector in December 2015 and December 2016 and their implications to the reliable and safe operation of nuclear plants. As this paper is prepared for the American Nuclear Society, the focus is on U.S. organizations even though this paper applies to all international organizations.

2 I&C CYBER SECURITY

Presidential Policy Directive/PPD-41 (United States Cyber Incident Coordination) was issued July 26, 2016. [1] PPD41 defines a cyber incident as an event occurring on or conducted through a computer network that actually or imminently jeopardizes the integrity, confidentiality, or availability of computers, information or communications systems or networks, physical or virtual infrastructure controlled by computers or information systems, or information resident thereon. For purposes of this directive, a cyber incident may include a vulnerability in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source. The PPD41 definitions are based on the traditional IT cyber security CIA (Confidentiality, Integrity, Availability) triad - where S (safety) is not considered and the term "malicious" is not used. Moreover, since there are minimal control system cyber forensics and often the only difference may be motivation, it may not be possible to distinguish an unintentional cyber incident from a malicious cyber attack. The 2008 Florida outage affected 26 transmission lines, 38 substations, caused a loss-of-offsite power (LOOP) automatic scram of the Turkey Point nuclear units, and left almost 3 million people without power for about 8 hours. The only difference between this incident being malicious or unintentional was the motivation of the person involved [2] (the impact is similar to the 2015 Ukrainian hack). In the case of the 2008 Florida outage, the threat source was the SCADA operator taking actions based on incomplete information. Moreover, control system cyber incidents can, and have, resulted in injuries and deaths – more than 1,000 deaths to date.

Instrumentation and control (I&C) cyber security addresses the unique issues associated with the cyber security of I&C systems. That is, I&C cyber security consists of protecting the reliability and safety of I&C systems from cyber threats, whether those threats have a malicious or involuntary origin. I&C cyber security also addresses cyber issues that may not be network-related but directly affect the field devices such as cyber threats to protective relays. Consequently, I&C cyber security is technologically, administratively, and procedurally different than cyber security of Information technology (IT) business systems [1]. One of the more glaring differences between IT and I&C cyber security is the lack of control system cyber forensics at the sensor and actuator layer (Level 0,1 in the Purdue Reference Model) [3]. The lack of I&C cyber forensics and the lack of appropriate I&C cyber security training has resulted in the lack of identifying actual control system cyber incidents as being cyber-related. As a result of this shortcoming, in June 2015 I provided Scenario-Based Training to the International Atomic Energy Agency (IAEA) on three selected nuclear plant I&C cyber incidents. [4] These incidents were:

- not identified as cyber,
- affected safety systems used in nuclear power plants even though the initiating systems were not safety-related, and
- caused by I&C-specific issues not IT-network related issues.

One of the selected incidents involved digital protective relay issues in the switchyard that caused LOOP events after every scram yet was not identified as being cyber-related.

3 CYBER THREATS AND ATTACKS AGAINST THE U.S. ELECTRIC GRID

The U.S. and other countries' electric grids are composed of cyber vulnerable I&C equipment including Supervisory Control and Data Acquisition (SCADA) master stations, Remote Terminal Units (RTUs), Intelligent Electronic Devices (digital protective relays), electrical instrumentation including current and potential transformers, and process sensing including temperature, humidity, voltage, and current sensors. The Ethernet networks and associated equipment used for the control system networks such as gateways, routers, and switches have been shown to have cyber vulnerabilities as seen by the numerous vulnerability disclosures for the different vendors. Additionally, there has been a lack of appropriate control system cyber security training and lack of adequate control system cyber security policies. As a result, there have been many actual control system cyber incidents. To date, the author has

been able to amass a database of more than 900 unintentional and malicious I&C cyber incidents in all industries including nuclear plants with more than 250 I&C cyber incidents in the North American Electric industry. These cyber vulnerabilities, combined with lack of appropriate training and sophisticated dedicated attackers, creates a dire situation.

Moreover, as identified by the U.S. Department of Homeland Security in the May/June 2015 DHS Monitor, [5] the U.S. electric grids have already been compromised with a variant of the BlackEnergy malware [6] used in the Ukrainian cyber attacks. Specifically, the 2015 DHS ICS CERT Monitor stated: "Some asset owners may have missed the memo about disconnecting control system from the Internet. Our recent experience in responding to organizations compromised during the BlackEnergy malware campaign continues to bring to light this major cyber security issue—Internet connected industrial control systems get compromised. All infected victims of the BlackEnergy campaign had their control system directly facing the Internet without properly implemented security measures. The BlackEnergy campaign took advantage of Internet connected ICS by exploiting previously unknown vulnerabilities in those devices in order to download malware directly into the control environment. Once inside the network, the threat actors added remote access tools, along with other capabilities to steal credentials and collect data about the network. With this level of access, the threat actor would have the capability to manipulate the control system." As noted in the next session, this was the approach used in the 2015 Ukrainian cyber attack.

Additionally, in 2015, NATO discussed Russian cyber threats against control systems in "Beyond 'Cyber War': Russia's Use of Strategic Cyber Espionage and Information Operations in Ukraine" by Jen Weedon. According to Jan, "Is Russia preparing for future cyber attacks on Western critical infrastructure? This is difficult to prove, but the Sandworm group has reportedly targeted supervisory control and data acquisition (SCADA) equipment, which is used in industrial and critical infrastructure settings, with the BlackEnergy toolkit. The victims were production systems, not vendor-owned prototypes or systems that contained financial information, intellectual property, or political intelligence. Given the targets seemed to be production systems, there would likely be no benefit from an espionage perspective to infect these systems. Rather, the actors using the malware may have been looking for weaknesses to exploit in a future disruptive scenario. In addition, the use of a crimeware toolkit offers a degree of anonymity or plausible deniability for actors with more destructive purposes."[7]

4 2015 AND 2016 UKRAINIAN CYBER ATTACKS

December 23, 2015 cyber attacks targeted three power distribution companies in the West of the Ukraine. December 20, 2016 cyber attacks targeted the transmission system in Kiev. There were similarities in both cyber attacks and each remotely opened substation breakers causing power outages. Additionally both cyber attacks did NOT attempt to remotely reclose the breakers that would have caused an Aurora event (see Section 5.3). It is not clear why the attackers did not reclose the breakers as the Aurora information was declassified and publicly available.

4.1 The 2015 Attack [8]

Although the attacks were triggered on December 23rd, 2015, the attacks were carefully planned with the networks and systems compromised as early as eight months earlier. In the 2015 attack, the targeted utilities had proper firewalls setup, one between the IT and the Internet and the second between the IT and OT (control system) network. The OT network included a DMS (Distribution Management System) SCADA with servers and workstations, gateways used to send orders from the DMS to remote RTUs that controlled the substation breakers, and other equipment in the electrical substations. In May 2014, the attackers targeted a Ukrainian electricity distributor in a phishing campaign using weaponized Microsoft Word documents. The attackers forged the sender addresses and weaponized the Microsoft word

attachments by using droppers to deliver the BlackEnergy Remote Access Trojan (RAT). In March 2015, the attackers began a wide-reaching phishing campaign that exploited a zero-day vulnerability to deliver a variant of the BlackEnergy malware to targeted systems. The attackers were able to install the BlackEnergy RAT after employees from each of the three distribution utilities opened the weaponized email attachments. During the next several months the BlackEnergy malware was remotely controlled to collect data, moved from one host to another, detected vulnerabilities, and made its way onto the OT network and perform similar "reconnaissance" activities. Forensic data analysis about this phase is incomplete, as the attacker wiped several disks during the actual attack. In the June to December 2015 time frame, the attackers used the BlackEnergy RAT to gather stored credentials and logged keystrokes. This enabled the attackers to create new privileged accounts and had the compromised system blend into normal network traffic. The attackers were able to enumerate systems deployed across the network, identified targets, and began preparations for the final attack. Prescheduling execution of malware enabled coordination of multiple attack components, such that data destruction coincided with, or shortly followed attacks against the substation breakers. Critical systems were targeted to shut down as a result of the power outages that would impact restoration efforts. Finally, the attackers used valid credentials to seize control of operator workstations, accessed DMS client applications via a VPN, and issued unauthorized commands that opened breakers at the substations. After opening the breakers, the attackers delivered malicious firmware updates to serial-to-Ethernet converters. The malicious updates rendered the converters inoperable and severed the connection between the control center and the substations. The attackers then used network access to schedule the temporary backup power to be offline at the time of the power outages that impacted operation of critical systems. The disruption at the data center associated reboot triggered execution of Killdisk malware that prevented adequate forensics. Despite the more advanced stage of IT cyber security, Ethernet network cyber vulnerabilities and malware existed for months before they were identified in both the 2015 and 2016 attacks.

4.2 The 2016 Attack [9]

There is not the same level of detail about the December 2016 attack yet. However, what is known is the 2016 cyber attacks remotely opened transmission station breakers. Additionally the 2016 attacks were more complex and better organized. The malware in the 2016 attack had more obfuscation and was adapting to cyber security defenses including firewalls. As with the 2015 cyber attacks, the 2016 cyber attacks went undiscovered for months.

5 IMPLICATIONS TO NUCLEAR POWER PLANTS

There were several protective relay issues from the Ukrainian attacks that could affect nuclear plant operations: (1) compromised relay operation preventing the protective trip function from actuating; (2) compromised relay operation causing unexpected relay tripping resulting in LOOP conditions; and, (3) reclosing of the protective relays out-of-phase with the grid (the Aurora vulnerability) which has been demonstrated to have severe equipment damage. All of these threats can originate from "outside the fence". That is, the initiating event is from outside the reactor building starting either in the plant switchyard or an external substation outside the plant fenced-in area that may not even be owned by the nuclear plant's operator. Regulatory Guide 5.71, C.7 Defense-in-Depth [10] states that any non-safety system that has bi-directional communication to a safety system is afforded the same level of protection as the safety system. However, the switchyard and the neighboring substation are not included. Additionally neither Regulatory Guide 5.71 nor NEI-0809 specifically identify protective relays. Consequently, these originating sources would be outside the scope of Regulatory Guide 5.71 and NEI -0809 [11]. There is one other issue about an attack originating from a protective relay. That is, it would be irrelevant whether the nuclear plant system that would be impacted would have analog or digital I&C because the impact is upstream of the I&C.

Protective relays are critical to the operation of the electric grid and the protection of large electric equipment in many industries including electric, nuclear, manufacturing, etc. Protective relays are used to protect electric equipment such as motors and generators from faults such as overcurrent, under/over voltage and under/over frequency. Protective relays were originally electro-mechanical switches but have progressed to complex networked digital devices with enormous computing capabilities making them intelligent electronic devices (IEDs). Consequently, IEDs are now cyber vulnerable from both IT network and control system issues. Digital protective relays provide a higher level of reliability, more functionality, and the ability to provide direct integration into multiple devices including SCADA compared to the older mechanical protective relays. Consequently, digital protective relays are an integral part of grid and plant modernization including nuclear plants. Where IEDs can be compromised physically and remotely, analog control systems in distribution substations and transmission stations can be physically compromised leading to damage of equipment served by those stations. This is important to mention in order to understand how critical control systems are to electric facilities.

When a relay fails to operate as designed, major equipment damage or failure can occur with little opportunity to prevent the event because it was the protection that was compromised. An example of this was presented at the 2106 ICS Cyber Security Conference [12] where an industry-standard relay was compromised (Figure 1).

Figure 1. Hack of a Protective Relay

5.1 Compromised Relay Operation (Failure to Trip)

As mentioned, protective relays are critical to the operation of the electric grid and the protection of large electric equipment in many industries including electric, nuclear, manufacturing, etc. Protective relays monitor many critical electric parameters including current, voltage, and frequency. The relays then issue a trip command in milliseconds when a setpoint is reached to protect the equipment. If the relay is compromised and a trip command is not issued, large critical electric equipment can be damaged.

5.2 Loss-of-Offsite (LOOP) Conditions (Erroneous Trip)

Remotely opening protective relays can cause outages that lead to nuclear plant scrams from loss-of-offsite power (LOOP). This occurred with the 2003 Northeast Outage and then with the 2008 Florida outage. U.S. nuclear regulations allow for 2-3 operational transients/year as this may account for electrical or mechanical failures, or even weather conditions. As an example, on December 18, 2016, the Columbia nuclear power plant experienced a full reactor scram and did not return to full power until December 28.

Preliminary investigations indicate that the scram was caused by a load reject from the Bonneville Power Administration Ashe substation (Figure 2).

Figure 2. Bonneville Power Administration's Ashe Substation

Equipment malfunctioned at the substation resulting in a loss of the 500KV line connecting to Columbia's main output transformers to Ashe. Columbia experienced a complete loss of the reactor closed cooling system, a reactor high pressure trip, a 13-inch increase in reactor water level activations, and the closing of the main steam isolation valves, among other conditions. The reactor core isolation cooling and high pressure core spray were manually activated and utilized to maintain reactor water level. [13 and 14] This incident could have been caused by compromising the protective relays at the Ashe substation which is neither owned nor controlled by the Columbia nuclear plant.

However, the regulations allowing for the 2-3 operational transients/year were not meant to address malicious attacks where plant equipment could undergo for example 2-3 operational transients/month. Hackers having the ability to open substation protective relays can potentially create this type of situation as demonstrated by the 2008 Florida outage, the 2016 Columbia nuclear plant scram, or the malicious 2015 and 2016 Ukrainian cyber attacks.

5.3 The Aurora Vulnerability [15]

Out-of-phase conditions and grid synchronization issues have been discussed for more than 50 years. Reference 13 discusses the technical issues for out-of-phase damage to critical electric equipment. This paper was based on unintentional considerations as malicious issues were simply not considered.

The Aurora Generator Test (or simply the "Aurora Test) is the name for a class of power line attacks that manipulate physical forces to cause damage through industrial automation controllers. The basis behind Aurora is a well-known issue that is taught to first year electrical engineering students –don't start Alternating Current (AC) equipment out-of-phase with the electric grid. In September 2006, a university/national laboratory whitepaper dealing with out-of-phase conditions was presented at a conference partially sponsored by China. The out-of-phase condition can occur unintentionally or maliciously (Aurora). On April 14, 1949, TVA's Ocoee No. 2, Unit #2 suffered a hydro generator failure. With the synchronizing (sync) check relay unintentionally wired out-of-phase, the generator turbine broke through the generator building and ended up about a 1/4 mile away (Figure 3) [16]

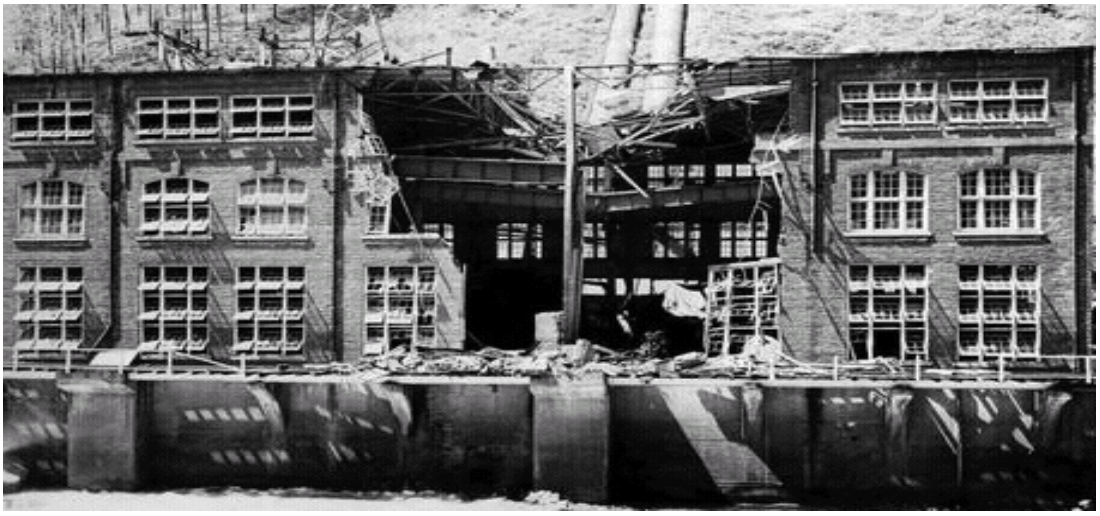

Figure 3. TVA Ocoee Unit 2 Failure

A more recent case was another utility that unintentionally wired the generation step-up (GSU) transformer sync check relay out-of-phase. When the transformer was energized after maintenance, high transient currents and mechanical stresses destroyed the transformer and spilled transformer oil in the environment. GSUs are multi-million dollar devices that can take more than 9 months to build with very few spares available. When these devices are unavailable, a power plant is effectively useless. What is novel about Aurora is the ability to maliciously and remotely cause the out-of-phase condition.

Aurora dates from 2006 when the Idaho National Laboratory (INL) requested DHS funding for an Aurora demonstration project. In October 2006, INL completed the real time power system simulations demonstrating the physics and in November 2006 demonstrated the validity of the vulnerability against a 15 Horsepower (hp) generator/induction motor. In responding to a request from the Secretary of DHS, INL hired experts to verify and configure the test with NERC participation. In March 2007, INL performed the test against the 2.1 MW generator. (Figure 4).

Figure 4. The March 2007 Aurora Test

The results of the test were initially provided to industry by DHS at a closed door session March 7, 2007 at the Spring 2007 DHS Process Control Security Forum (PCSF) Conference. However, due to the lack of clear (and often conflicting) information about the test and the fear of NERC CIP audits, a de facto assessment was made by the industry that there was minimal risk from Aurora. Further speculation by industry was that such a vector would not be able to be weaponized by a hacker for 5-7 years. However, evidence implies this cyber path has been exploited since 2009. October 13, 2010 NERC issued a second NERC Advisory on Aurora. This advisory did not require any hardware mitigation either. In April 2011, Dominion Electric and Quanta issued an IEEE paper that attempted to demonstrate that the existing Aurora hardware mitigation would cause grid reliability problems. Unfortunately, the paper's assumptions were

flawed and also mischaracterized what actually occurred at the INL test. In March 2012, DOD and a small electric utility with no NERC critical cyber assets initiated the first project on Aurora hardware mitigation. In July 2013, a second utility, also with no NERC critical cyber assets, initiated a project with DOD on Aurora hardware mitigation.

Aurora exploits a physical gap in relay protection of the electric grid that affects EVERY substation without specific Aurora hardware mitigation. The impact is on the loads connected to the substation such as nuclear plants or other industrial or commercial facilities. Aurora does not even have to be initiated at the substation adjacent to the load (i.e., nuclear plant) but can be the next nearest substation. As best as the Author can tell, there have already been Aurora attacks though they are not publicly acknowledged.

The lack of protection can be seen from the Current and Voltage Protection functions that are either not applicable (don't react to Aurora conditions) or too slow to protect against the reclose out-of-phase condition (Table I).

Table I. Current and voltage generator protection functions to address Aurora

Description	Operate during Aurora Conditions (Y/N)	Comments
Overcurrent	Y	Too slow
Directional	Y	Too slow
Distance	N	
Current Balance	N	
Reverse Power	Y (Diesel)	Too slow
Differential	N	
Loss of Excitation	N	
Overvoltage	Y	Too slow
Undervoltage	N	
Ground Overvoltage	N	
Voltage Balance	N	
Over/Under Frequency	Y	Too slow

5.3.1 INL Aurora test results

The INL test used a 2.1 MW generator (Figure 4). The generator suffered extensive physical damage with 14 of 16 engine cylinders destroyed, engine-to-generator coupler shredded, and engine bearing material dispersed. The accelerometer recoded a peak torque of more than 25 Gs (3-5 times normal). The first sign of damage occurred after the first hit with destruction after multiple hits. The system dispatcher reported he could not see any external effects until the generator was effectively destroyed and off-line. This indicates that reliability-centered maintenance (RCM) programs that were assumed to be able to detect loss of equipment life can be unknowingly compromised with significant damage that has not been identified. The control breaker functioned properly through each attack cycle and sustained no damage. The results were representative of results expected by industry representatives and matched the pre-test simulation results.

5.3.2 How the Ukrainian cyber attacks would affect an Aurora event

Equipment: a device that is able to open/close breakers. For a cyber attack, that would be a device (e.g., laptop, desktop, cell phone, dial-up modem) with remote connection to the breakers. These devices are used in many nuclear plants. *This access was available in both Ukrainian cyber attacks*.

Access: Physically through the front panel or remotely through dial-up modem, Internet, wireless, hand-held, or SCADA. *This occurred in both Ukrainian cyber attacks*.

Knowledge: In order to maximize the impact of the attack, detailed power engineering knowledge with relay device setting skills are necessary. This would include equipment manuals and default passwords which are generally known and available throughout the industry. Hacking skills are needed to exploit the ICS and conduct the attack. *This obviously occurred with both Ukrainian cyber attacks*.

Time: The time to cause the Aurora event takes less than a minute. Because the impact occurs so rapidly, timing is not critical for degrading or destroying equipment. Cyber can not only cause the initial initiation but can cause additional Aurora events on any desired schedule. Having the ability to remotely open breakers allows the hackers the ability to cause an Aurora event in their time of choosing if there is no appropriate Aurora hardware mitigation. *This would apply to the Ukrainian cyber attacks.*

6 RECOMMENDATIONS

The following recommendations are suggested to minimize the potential impacts of a grid cyber attack affecting nuclear plant operation:

- Regulatory Guide 5.71 and NEI-0809 need to be modified for addressing protective relays.
- The U.S. Federal Energy Regulatory Commission (FERC) needs to coordinate with the U.S. NRC on grid cyber attacks that could affect nuclear plants. FERC also needs to require that the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) standards address the cyber security of the substations and protective relays that could affect nuclear plants. In addition NERC needs to intensify its enforcement of its Protection and Control Standards (PRC) specifically PRC-005 Protection System Maintenance and PRC-019 Coordination of Generating Unit or Plant Capabilities, Voltage Regulating Controls, and Protection, which were cited as part of a group of most violated standards in its Compliance Monitoring and Enforcement Reports for 2016 [18].
- Employ Aurora hardware mitigation disconnected from any Ethernet network.
- Employ state-of-the-art cyber network monitoring and anomaly detection.
- Provide control system cyber security training for control system personnel, substation personnel, and IT security personnel to be able to identify potential cyber-related incidents.

7 CONCLUSIONS

Studies, demonstrations, and the 2015 and 2016 Ukrainian cyber attacks, have shown that nuclear plants can be adversely impacted by grid cyber attacks. Cyber attacks from outside the plant buildings (switchyards and substations) are outside existing regulatory scope even thou it has been shown that substation relay operation can have detrimental impacts on nuclear plant operation. Malware exists in the U.S. grids that can be used to compromise protective relay operation. There are appropriate hardware and training approaches to minimize the plant impacts from potential grid cyber incidents, but they need to be applied. Protecting nuclear plants from grid cyber attack will also require that regulations specifically address these currently out-of-scope events.

ACKNOWLEDGMENTS

The descriptions of the 2015 Ukrainian cyber attack was drawn from several sources particularly the BoozAllen Hamilton report – When the Lights Went Out. Details from the 2016 Ukrainian cyber attack are still not publicly available so the information was drawn from a presentation at the January 2017 S4

Conference. Michael Swearingen provided input on protective relays issues including NERC protective relay compliance issues.

REFERENCES

1. Presidential Policy Directive -41, http://www.controlglobal.com/blogs/unfettered/presidential-policy-directive-41-does-not-require-cyber-incidents-to-be-malicious-or-affect-safety/
2. Joseph Weiss, *Protecting Industrial Control Systems from Electronic Threats*, May 2010, Momentum Press, ISBN: 978-1-60650-197-9.
3. Theodore J. Williams, *The Purdue enterprise reference architecture: a technical guide for CIM planning and implementation*. Research Triangle Park, NC: Instrument Society of America, 1992.
4. Weiss, Joe, "Scenario-Based Training for Nuclear Power Plants", presentation to the International Atomic Energy Commission, June 4, 2015.
5. ICS Monitor May, June 2015, "If you're Connected, Your Likely Infected!", https://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_May-Jun2015.pdf
6. BlackEnergy, Intel report, https://www.mcafee.com/threat-intelligence/malware/default.aspx?id=260171
7. Joe Weiss, http://www.controlglobal.com/blogs/unfettered/the-burlington-electric-department-cyber-attack-story-has-been-misreported-even-though-malware-is-in-our-us-electric-grids/, 1/2/17
8. "When the Lights Went Out, A Comprehensive Review of the 2015 Attacks on Ukrainian Critical Infrastructures", Booz Allen Hamilton, September 2016.
9. Mariana Krotofil, Cyber Attacks on Ukraine Power and Critical Infrastructure, https://www.youtube.com/watch?v=lTwsDLO3C44&feature=youtu.be&utm_content=buffer7ab12&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer
10. Regulatory Guide 5.71, Cyber Security Program for Nuclear Power Plants, January 2010.
11. NEI-0809, Cyber Security Plan for Nuclear Power Reactors, Rev 6, April 2010.
12. 2016 ICS Cyber Security Conference – www.icscybersecurityconference.com
13. "End of year brings one scram, one trip", Nuclear News, February 2017, P.24.
14. NRC LER Number 397-2016-004, Automatic Scram Due to Off-Site Load Reject
15. Michael Swearingen, Steven Brunasso, Joe Weiss, and Dennis Huber, "What You Need to Know (and Don't) about the Aurora Vulnerability", Power, September 2013, P.52-56
16. Thomas Beckwith, "Automatic Synchronizing Considerations and Methods", Western Protective Relay Conference, October 23, 1985
17. IEEE Tutorial on the Protection of Synchronous Generators, Second Edition 2011, Special Publication of the IEEE Power Systems Relay Committee.
18. NERC Compliance Monitoring and Enforcement Program Report, Q3, 2016, November 1, 2016

APPENDIX A

For further reading, the following are recommended:

- Ellen Smith, Scott Corzine, Donald Racey, Patrick Dunne, Colin Hassett, Joe Weiss, “Going Beyond Cybersecurity Compliance”, IEEE Power and Energy, September/October 2016, P.48-56
- Weiss, Joe, presentation to the National Academy of Science, Engineering, and Medicine Government-University-Industry Research RoundTable (GUIRR), Critical Infrastructure Security: The Role of Public-Private Partnerships, “Cyber security of Industrial Control Systems” February 23, 2016 http://sites.nationalacademies.org/PGA/guirr/PGA_171115