Cybersecurity Standards and the 2015 Ukraine Power Grid Attack:

Mitigating Catastrophic Cyber Disruptions on Electrical Infrastructure

By Sam Cohen
Missouri State University DC Graduate Campus
Georgetown University

Abstract: The 2015 attack on Ukraine's power grid represented the first publically documented cyber incident disrupting electrical utility and power distribution control systems. While the incident was temporary, it impacted critical services supporting 225,000 customers—including businesses, industrial facilities, and government offices. The attack has been recognized as a highly complex and persistent operation that could have escalated to a significantly larger power outage disaster, threatening long-term essential service disruptions at hospitals, government facilities, telecommunication sites, and financial institutions. This paper examines how cybersecurity standards developed or approved by organizations such as the National Institute for Standards and Technology (NIST), the American National Standards Institute (ANSI), the International Organization for Standardization (ISO), the North American Electric Reliability Corporation (NERC), and the International Electrotechnical Commission (IEC) could have either mitigated or entirely prevented this attack. Specifically, log collection and analysis (NERC CIP-007-6 and NIST SP-800-92), external network and boundary protection (IEC 62443-3, adopted as ANSI/ISA 99.03.03), and incident response (NIST-7628 Rev.1 and ISO/IEC 27002:2013) standards are mapped against key cybersecurity gaps that enabled the attackers to compromise and exploit key assets throughout Ukraine. The paper then determines how controls listed in these standards could have assisted cybersecurity and IT staff with the defense of their control systems and supervisory control and data acquisition (SCADA) networks, thereby reducing the destructive potential of the attack and possibly mitigating the disaster altogether. The standards analyzed in this paper are identified for their mitigation utility during the Ukraine attacks, and also for their applicability to any power grid owner or operator aiming to reduce cyber risk.

Introduction and Overview

On December 23, 2015, regional electrical grids in three Ukrainian provinces experienced operational downtime for nearly six hours, impacting power supply to 225,000 customers.[1] Government offices, industrial facilities, business centers, and private residences were affected.

[1] Kevin Owens et al., "Ukraine Cyber-Induced Power Outage: Analysis And Practical Mitigation Strategies," *Schweitzer Engineering Laboratories, Inc.* (paper presented at the Power and Energy Automation Conference, Spokane, Washington, March 21, 2017), 1-2. https://www.eiseverywhere.com/file_uploads/aed4bc20e84d2839b83c18b cba7e2876_Owens1.pdf.

After initial digital forensic investigations and root-cause analysis were complete, government and private cybersecurity stakeholders recognized that this incident was the result of a coordinated and comprehensive cyber attack. The impact of this attack was both financially costly and strategically significant, as it represented an evolution in the use of cyberspace for kinetic effects in addition to forcing Ukrainian power utilities to incur years of information technology repairs and large investment in new equipment replacements.

Not only are cyber threats to power grid critical infrastructure assets a core concern for national security, but they also represent a fundamental risk to businesses and organizations that rely on the uninterrupted daily distribution of their services—such as hospitals and water distribution centers requiring constant access to electricity. For example, a disruption equal to or greater in scale than the 2015 Ukraine incident near a major urban financial center inside the U.S. could temporarily shut down banks, international business headquarters, and telecommunication networks supporting money lending and transaction markets.[2] This could induce a regional or national liquidity disaster, adversely influencing economic activity and halting money market operations. A 2018 International Monetary Fund report titled "Cyber Risk for the Financial Sector" reinforced this perspective, noting that, "The disruption of material infrastructures such as power grids and IT infrastructures could also have a large macroeconomic impact. Recent studies estimate that a disruption of part of the U.S. power grid could lead to up to USD 1 trillion in losses."[3] In 2017, the U.S.-based Council on Foreign Relation raised urgency to this power grid cybersecurity threat, highlighting that, "Rapid digitization combined with low levels of investment

[2] Carolyn Cohn, "Cyber attack on U.S. power grid could cost economy $1 trillion: report," *Reuters*, https://www.reuters.com/article/us-cyberattack-power-survey/cyber-attack-on-u-s-power-grid-could-cost-economy-1-trillion-report-idUSKCN0PI0XS20150708.

[3] Antoine Bouveret, "Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment," *International Monetary Fund: Working Paper Series* wp.18 no. 143 (2018), 11-12.

in cybersecurity and a weak regulatory regime suggest that the U.S. power system is as vulnerable—if not more vulnerable—to a cyberattack as systems in other parts of the world."[4]

Considering the scale and potential impact a major cyber incident could pose to the electrical grid inside the U.S. and across many other partner countries around the world, it is important to identify how the 2015 Ukraine incident could have either been mitigated or more effectively contained. This is particularly relevant as foreign and domestic threat actors—such as governments, hacktivists, or insider threats—continue to rapidly improve their technical sophistication and capability to conduct sustained network exploitation activities on critical power infrastructure. Therefore, this paper will explore former and current power utility, smart grid, and critical infrastructure cybersecurity standards that could have either prevented or improved technical responses to the 2015 Ukraine electrical grid cyber attack.

Cybersecurity Standard Implementation as a Mitigation Strategy

NERC CIP-007-6 and NIST SP-800-92

The Energy Policy Act of 2005 gave the Federal Energy Regulatory Commission (FERC) authority to oversee mandatory reliability standards governing the nation's electricity grid.[5] This included authority to approve mandatory cybersecurity reliability standards ranging from technical industrial control system (ICS) software reviews to patch management policies for supervisory control and data acquisition (SCADA) systems. The first comprehensive power grid cybersecurity

[4] Robert W. Knake, "A Cyberattack on the U.S. Power Grid," *Council on Foreign Relations: Center for Preventative Action*, April 3, 2017, https://www.cfr.org/report/cyberattack-us-power-grid.

[5] Federal Energy Regulatory Commission Fact Sheet, "Energy Policy Act of 2005: Significant Policy Changes," August 8, 2006, https://www.ferc.gov/legal/fed-sta/epact-fact-sheet.pdf.

policies—defined as Critical Infrastructure Protection (CIP) standards—were initially developed by the North American Electric Reliability Corporation (NERC) and approved by FERC in 2008.[6]

In March 2017, researchers from Schweitzer Engineering Laboratories, Inc., presented a report titled "Ukraine Cyber-Induced Power Outage: Analysis and Practical Mitigation Strategies" at the Power and Energy Automation Conference in Spokane, Washington.[7] The report notes that a lack of system logging and monitoring at power generation facilities contributed to the inability of IT and engineering teams to effectively implement an incident response plan. The report also highlights that this lack of logging control system network activity and the failure to establish standard baseline system data prevented cybersecurity emergency response teams from being able to effectively conduct root cause analysis of the cyber incident. This hindered initial investigations and digital forensics, which created a lasting issue for precisely determining what security controls and standards could have helped mitigate the attack. Nevertheless, recommendations from the 2017 report and from a cybersecurity study produced by the Electricity Information Sharing and Analysis Center (E-ISAC) in 2016 explicitly state that comprehensive logging and monitoring—in addition to automated correlation—were necessary components of an effective cybersecurity posture that an electric facility relying on SCADA and ICS networks should have included.[8]

To mitigate the logging issue at the Ukrainian power facilities and other possible grid targets in the U.S. or abroad in the future, cybersecurity and executive management teams could have implemented NERC's CIP-007-6 Systems Security Management Standard. CIP-007-6

[6] Anastasios Arampatzi, "Revised Critical Infrastructure Protection Reliability Standard CIP–003–7: What Are the Changes?" *Trip Wire: The State of Security*, September 10, 2018, https://www.tripwire.com/state-of-security/regulatory-compliance/nerc-cip/revised-critical-infrastructure-protection-reliability-standard-cip-003-7-what-are-the-changes/.

[7] Owens et al., "Ukraine Cyber-Induced Power Outage: Analysis And Practical Mitigation Strategies," 1-2.

[8] Robert M. Lee, Michael J. Assante and Tim Conway, "Analysis Of The Cyber Attack On The Ukrainian Power Grid: Defense Use Case," *Electricity Information Sharing and Analysis Center*, March 18, 2016, pg. 17, 21, https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf.

security guidelines and controls aim "to manage system security by specifying select technical, operational, and procedural requirements in support of protecting Bulk Electric System (BES) Cyber Systems against compromise that could lead to misoperation or instability."[9] This standard calls for the implementation of log and monitoring alert systems combined with a centralized security event monitoring system where log analysis can be performed from a top-down perspective. These capabilities, mandated by the CIP-007-6 standard, would have provided cybersecurity and IT staff at the Ukrainian facilities with more awareness of their control equipment behaviour and possibly led to the discovery of malicious cyber activity before systems were shutdown or disrupted beyond repair.

A National Institute of Standards and Technology (NIST) special publication, SP-800-92, outlines computer security standards and guidelines to "provide practical, real-world guidance on developing, implementing, and maintaining effective log management practices throughout an enterprise."[10] Use of this publication's guidance would have provided the impacted Ukrainian facilities and power distribution networks with a comprehensive monitoring capacity, procedures for automated system activity reviews, and a record of the cyber incident that could have enabled greater root cause analysis. A 2016 industry report from the cybersecurity firm FireEye reinforces the role implementation of this type of standard could have played in mitigating the cyber-induced disaster in Ukraine or a similar attack in the future, stating that, "Robust log collection and network traffic monitoring are the foundational components of a defensible ICS network. Failure to perform these essential security functions prevents timely detection, pre-emptive response, and

[9] "Programs, Departments and Standards: CIP-007-6," *North American Electric Reliability Corporation (NERC)*, accessed March 27, 2019, https://www.nerc.com/pa/Stand/Pages/CIP0076RI.aspx.

[10] Computer Security Resource Center, "Guide to Computer Security Log Management," *National Institute of Standards and Technology (NIST)*, last modified September 2006, https://csrc.nist.gov/publications/detail/sp/800-92/final.

accurate incident investigation."[11] The same year, a report from the World Energy Council also reinforced the role log controls listed in SP-800-92 and CIP-007-6 could have yielded during the Ukraine disaster, explaining that a comprehensive log analysis program searching for "malicious signatures could have helped detect the attack."[12]

IEC 62443-3, Adopted as ANSI/ISA 99.03.03

Another ICS cybersecurity standard that would have directly mitigated major aspects of the cyber attack on Ukrainian power grid facilities is IEC 62443-3. Developed by the International Electrotechnical Commission (IEC) and adopted by the International Society of Automation (ISA) as the American National Standard ANSI/ISA 99.03.03,[13] this document provides a mechanism for improving industrial automation and control system cybersecurity. ISA now works with the IEC to maintain the standard's international implementation and to conduct continuous reviews and updates.[14]

Sentryo, an industrial cybersecurity firm based in France, highlighted in their analysis of the 2015 Ukraine cyber attack that two key controls within the IEC 62443-3 standard—restricted data flows (RDF) and network zone boundary protection—were not adequately met by impacted facilities. The report notes that if RDF control 5.2 met a higher level of implementation, "the operator could have isolated the facilities at the very first signs of the attack, which would have

[11] Industry Intelligence Team, "Cyber Attacks On The Ukrainian Grid: What You Should Know," *FireEye*, pg. 2, 2016, https://www.fireeye.com/content/dam/fireeye-www/global/en/solutions/pdfs/fe-cyber-attacks-ukrainian-grid.pdf.

[12] "World Energy Perspectives: The Road to Resilience," *World Energy Council*, 2016, pg. 19, https://www.worldenergy.org/wp-content/uploads/2016/09/20160926_Resilience_Cyber_Full_Report_WEB-1.pdf.

[13] "ANSI/ISA-62443-3-3 (99.03.03)-2013 Security for industrial automation and control systems Part 3-3," *International Society of Automation (ISA)*, accessed April 7, 2019, https://www.isa.org/store/ansi/isa-62443-3-3-990303-2013-security-for-industrial-automation-and-control-systems-part-3-3-system-security-requirements-and-security-levels/116785.

[14] "New ISA/IEC 62443 standard specifies security capabilities for control system components," *International Society of Automation (ISA)*, accessed April 7, 2019, https://www.isa.org/intech/201810standards/.

stopped the attack de facto."[15] These controls would have also increased monitoring of communications at the external boundary of important ICS tools controlling power distribution, thereby raising the prospect of detecting the attacker's use of malicious and unauthorized commands to turn multiple substations offline. IEC 62443-3 is another example of a technical standard capable of mitigating at least one key segment of the Ukraine cyber incident that enabled the overall attack. Further, it acts as a use case for other electric enterprises aiming to improve their cybersecurity posture with standards to prevent future disasters.

NIST-7628 Rev.1 and ISO/IEC 27002:2013

NIST-7628 Revision 1, referred to as "Guidelines for Smart Grid Cybersecurity," provides a high-level framework and standards-based recommendations for an overall smart grid cybersecurity strategy and policy architecture.[16] Certain comprised IT assets and ICS technologies at the impacted Ukraine facilities' relied on the smart grid digital networking approach to manage power supply provision to their customers. While these digital systems created financial and operational efficiency benefits from a management perspective, they also created technical IT vulnerabilities that the attackers specifically leveraged. This included identifying unique gaps in organizational incident response plans during network reconnaissance activities leading up to the main attack.[17] They aimed to ensure industrial control networks and human-machine interface workstations would not be brought back online once the primary shutdown commenced—

[15] Patrice Bock, "Analysis of cyberattack against Ukraine's power grid on December 23, 2015," *Sentryo*, July 18, 2017, https://www.sentryo.net/analysis-cyberattack-ukraine-power-grid/.

[16] National Institute of Standards and Technology (NIST), "Guidelines for Smart Grid Cybersecurity: Volume 1 - Smart Grid Cybersecurity Strategy, Architecture, and High-Level Requirements," *Department of Commerce*, September 2014, pg. 146, https://nvlpubs.nist.gov/nistpubs/ir/2014/NIST.IR.7628r1.pdf.

[17] Lee, "Analysis Of The Cyber Attack On The Ukrainian Power Grid: Defense Use Case," 5-6.

effectively disabling the digital linkages that make a smart grid effective for oversight and operational control.

Considering incident response was a fundamental challenge that ultimately enabled the success of the attack, there is a clear opportunity to apply the eleven NIST-7628 Rev.1 Smart Grid Incident Response (SG.IR) controls. It is also worth noting that the controls associated with information security management systems (ISMS) outlined in ISO/IEC 27002:2013—a standard jointly developed by the International Organization for Standardization (ISO) and the IEC—can provide similar useful incident response guidelines. For example, like the NIST-7628 Rev.1 guidelines, ISO/IEC 27002:2013 suggests the development and thorough testing of reporting, forensic incident collection, business continuity, and event analysis procedures.[18]

The previously mentioned 2016 E-ISAC study suggests that the Ukrainian network defenders at the facilities needed to "develop anticipatory responses to attack effects" and to add routine audits to "examine their detection and response capabilities."[19] During the power shutdown, attackers targeted server and computer uninterruptable power backup supplies (UPS) to ensure operators and IT staff could not conduct their established incident response procedures. The attackers also conducted a Telephony Denial of Service (TDoS) operation to disrupt the communications between in-house staff, external private firms, and government offices working to mitigate the attack.[20] This operation leveraged the same tactics of a Distributed DoS attack on network or application servers but aimed to overload the phone systems to disrupt emergency response coordination. Using the 11 NIST-7628 Rev.1 SG.IR controls, Ukrainian grid

[18] Eric Lachapelle and Mustafe Bislimi, "Whitepaper: ISO/IEC 27002:2013 Information Technology and Security Techniques," *ZIH and Professional Evaluation and Certification Board (PECB)*, February 26, 2016, pg. 9-10, http://zih.hr/sites/zih.hr/files/cr-collections/3/iso27002.pdf.

[19] Ibid., 15-16.

[20] Owens et al., "Ukraine Cyber-Induced Power Outage: Analysis And Practical Mitigation Strategies," 1.

cybersecurity teams would have had well-defined roles and responsibilities; tested response plans; outlined incident handling, monitoring, and reporting requirements; established incident investigation and analysis plans; and pre-designated system backup and emergency communication procedures.[21] According to the E-ISAC report, these capabilities could have directly identified the need for secondary capabilities at telecommunication sites to offset an active TDoS attack or the need to disable remote interactive functionality with field devices connected to SCADA grid information systems—a security gap the attackers used to shutdown electricity substations while masking themselves as authentic users. Therefore, use of the NIST-7628 Rev.1 controls—layered with the ISO/IEC 27002:2013 guidelines—would have directly provided a higher degree of cyber resiliency for power enterprises who suffered outages during the attack.

Conclusion

Leveraging the cybersecurity standards and guidelines listed in this paper would have directly influenced the sequence of events during the 2015 Ukraine cyber attack, either providing Ukrainian cybersecurity and IT staff with additional functional control over their systems or the ability to deny the attackers an initiative altogether. While the direct impact of the Ukraine incident was limited in terms of being a prolonged national disaster, the attack reinforced growing concerns that strategic IT threats to national power grid systems exist—and that certain actors are technically capable of exploiting their vulnerabilities. Private and public critical infrastructure stakeholders operating within the power grid, especially those rolling out new IT systems for smart grid operations, need to recognize cybersecurity standards as a financially and operationally feasible countermeasure to power grid and utility cyber risk. In doing so, a catastrophic cyber

[21] National Institute of Standards and Technology (NIST), "Guidelines for Smart Grid Cybersecurity: Volume 1 - Smart Grid Cybersecurity Strategy, Architecture, and High-Level Requirements," 146.

disaster in the future will likely be mitigated or even prevented, just as it would have been in Ukraine.

Bibliography

Arampatzi, Anastasios. "Revised Critical Infrastructure Protection Reliability Standard CIP–003–7: What Are the Changes?" *Trip Wire: The State of Security*. September 10, 2018. https://www.tripwire.com/state-of-security/regulatory-compliance/nerc-cip/revised-critical-infrastructure-protection-reliability-standard-cip-003-7-what-are-the-changes/.

Bock, Patrice. "Analysis of cyberattack against Ukraine's power grid on December 23, 2015." *Sentryo*. July 18, 2017. https://www.sentryo.net/analysis-cyberattack-ukraine-power-grid/.

Bouveret, Antoine. "Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment." *International Monetary Fund: Working Paper Series* wp.18 no. 143 (2018), 1-28.

Cohn, Carolyn. "Cyber attack on U.S. power grid could cost economy $1 trillion: report." *Reuters*. https://www.reuters.com/article/us-cyberattack-power-survey/cyber-attack-on-u-s-power-grid-could-cost-economy-1-trillion-report-idUSKCN0PI0XS20150708.

Computer Security Resource Center. "Guide to Computer Security Log Management." *National Institute of Standards and Technology (NIST)*. Last modified September 2006. https://csrc.nist.gov/publications/detail/sp/800-92/final.

Federal Energy Regulatory Commission (FERC). "Cyber and Grid Security." Last modified April 2019. https://www.ferc.gov/industries/electric/indus-act/reliability/cybersecurity.asp.

Industry Intelligence Team. "Cyber Attacks On The Ukrainian Grid: What You Should Know." *FireEye*. 2016. https://www.fireeye.com/content/dam/fireeye-www/global/en/solutions/pdfs/fe-cyber-attacks-ukrainian-grid.pdf.

International Society of Automation (ISA). "ANSI/ISA-62443-3-3 (99.03.03)-2013 Security for industrial automation and control systems Part 3-3." Accessed April 7, 2019. https://www.isa.org/store/ansi/isa-62443-3-3-990303-2013-security-for-industrial-automation-and-control-systems-part-3-3-system-security-requirements-and-security-levels/116785.

International Society of Automation (ISA). "New ISA/IEC 62443 standard specifies security capabilities for control system components." Accessed April 7, 2019. https://www.isa.org/intech/201810standards/.

Knake, Robert W. "A Cyberattack on the U.S. Power Grid." *Council on Foreign Relations: Center for Preventative Action*. April 3, 2017. https://www.cfr.org/report/cyberattack-us-power-grid.

Lachapelle, Eric and Mustafe Bislimi. "Whitepaper: ISO/IEC 27002:2013 Information Technology and Security Techniques." *ZIH and Professional Evaluation and Certification*

Board (PECB). February 26, 2016. http://zih.hr/sites/zih.hr/files/cr-collections/3/iso27002.pdf.

Lee, Robert M., Michael J. Assante and Tim Conway. "Analysis Of The Cyber Attack On The Ukrainian Power Grid: Defense Use Case." *Electricity Information Sharing and Analysis Center*. March 18, 2016. https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf.

National Institute of Standards and Technology (NIST). "Guidelines for Smart Grid Cybersecurity: Volume 1 - Smart Grid Cybersecurity Strategy, Architecture, and High-Level Requirements." *Department of Commerce*. September 2014. https://nvlpubs.nist.gov/nistpubs/ir/2014/NIST.IR.7628r1.pdf.

North American Electric Reliability Corporation (NERC). "Programs, Departments and Standards: CIP-007-6." Accessed March 27, 2019. https://www.nerc.com/pa/Stand/Pages/CIP0076RI.aspx.

Owens, Kevin, David E. Whitehead, Dennis Gammel, and Jess Smith. "Ukraine Cyber-Induced Power Outage: Analysis And Practical Mitigation Strategies." *Schweitzer Engineering Laboratories, Inc.* Paper presented at the Power and Energy Automation Conference, Spokane, Washington, March 21, 2017. https://www.eiseverywhere.com/file_uploads/aed4bc20e84d2839b83c18bcba7e2876_Owens1.pdf.

World Energy Council. "World Energy Perspectives: The Road to Resilience." 2016. https://www.worldenergy.org/wp-content/uploads/2016/09/20160926_Resilience_Cyber_Full_Report_WEB-1.pdf.