SCADA Fusion With Commercial Fission

by Matthew Horner

Abstract

Nuclear power plants rely on digital components, like supervisory control and data acquisition (SCADA) devices, to perform daily operations. These devices can contain software vulnerabilities. To address SCADA and other cyber threats, the U.S. Nuclear Regulatory Commission (NRC) has issued directives for licensed operators to submit cybersecurity plans for their facilities. While the guidance is on par with other sectors, the application may be inadequate. Protection against cyber-attacks becomes more important as SCADA systems become more standardized and connected to other networks. In addition to resilient components, improvements like redundancy, whitelisting, and intrusion detection systems can help improve a SCADA network. Ultimately, the nuclear power industry may need to undergo a culture shift in order to reduce the vulnerability of these systems. An information- sharing and analysis center can also provide lessons learned and expertise to the NRC and nuclear power plants in the U.S.

Suggested Citation

Horner, Matthew. "SCADA Fusion With Commercial Fission." *Homeland Security Affairs* 14, Article 4 (April 2018). https://www.hsaj.org/articles/14317

Introduction

Like other power plants, nuclear power plants rely on digital components to perform daily operations. Many of these components are supervisory control and data acquisition (SCADA) devices that can contain software vulnerabilities.[1] The Nuclear Energy Institute (NEI) claims that "critical systems" in a nuclear reactor facility are not connected to the Internet or the facility's internal network and therefore that the cybersecurity risk to these critical systems is minimized.[2]

However, the stakes in nuclear power are always high. Not only do the facilities provide electricity to communities, but they also contain nuclear fuel. Accidents at nuclear power plants are well-publicized. Three Mile Island, Chernobyl, and Fukushima Daiichi are names that invoke the dangers of nuclear power, and they will likely not fade anytime soon. Additionally, terrorists can target nuclear power plants seeking to gain access to nuclear fuel to create a "dirty bomb," or an explosive device meant to spread radioactive particles over a large area.[3] Cyber-attacks add to the list of threats to a nuclear power plant, and they have the unique property of attacking from afar and anonymously. This paper will discuss SCADA systems in commercial nuclear power plants in the U.S., focusing on

- incorporation of digital and networked components in U.S. commercial nuclear power plants,
- a summary of policy for cybersecurity in nuclear power plants,
- cybersecurity threats to and vulnerabilities of nuclear power plants, and consequences of a successful exploitation, and
- recommendations to improve the cybersecurity of the nuclear power plant infrastructure.

Incorporation of Digital and Networked Components

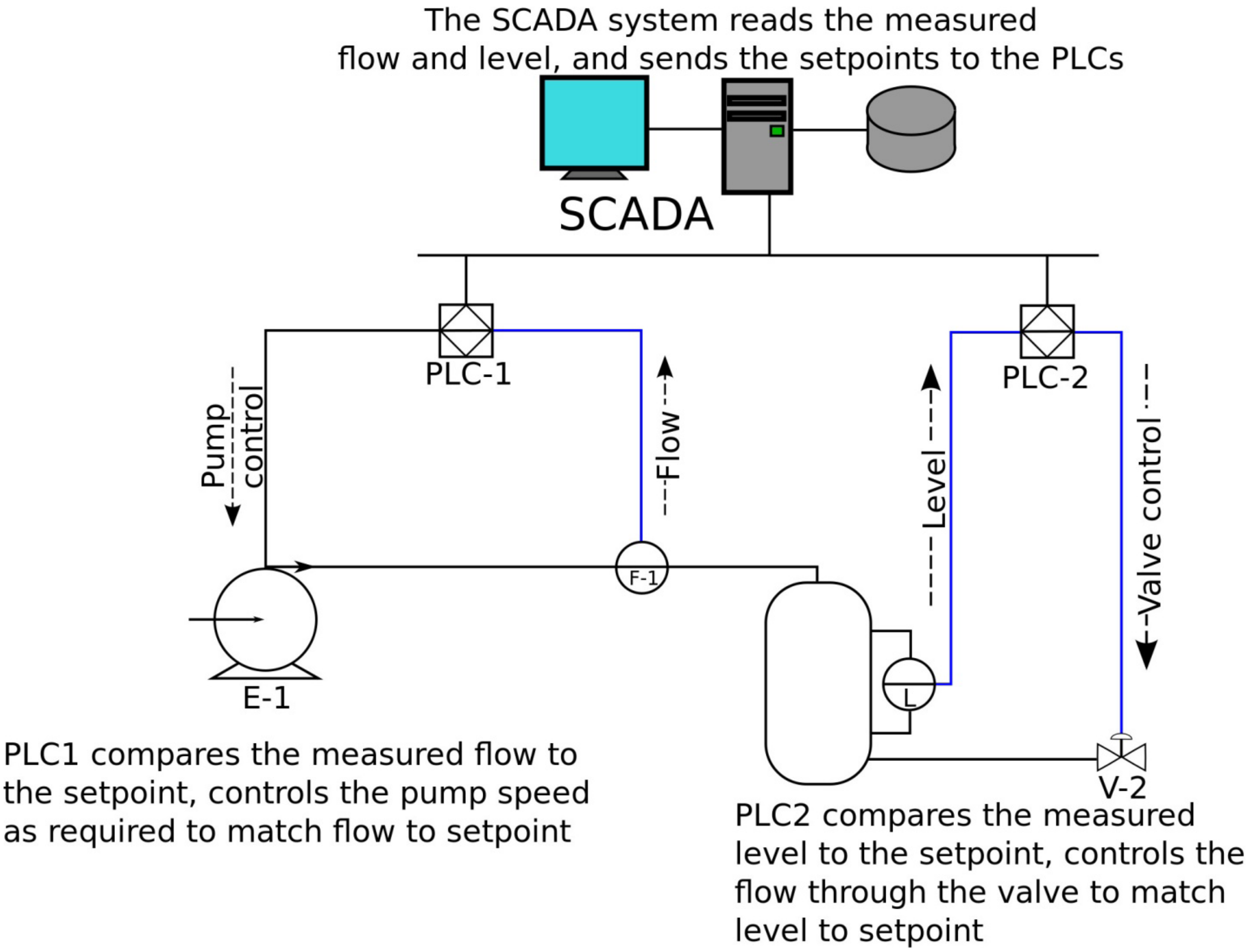
The Nuclear Reactors, Materials, and Waste Sector (or Nuclear Sector) of the U.S. is one of the 16 critical infrastructures (CI) as defined in Presidential Policy Directive-21.[4] A basic understanding of power plant construction and functionality is useful to help the reader appreciate the risk to this sector. Instead of burning fossil fuels, nuclear power relies on a process called fission which involves splitting atoms of a fissile material like Uranium-235. Fission creates thermal energy that can be used to generate electricity. However, it also produces radioactive elements that must be trapped within a containment barrier. If these radioactive elements are released, long-term environmental and public health consequences can result as seen in Chernobyl, Ukraine and Fukushima, Japan.[5] According to the Department of Homeland Security (DHS), the high-impact consequences of mishandling nuclear assets make the Nuclear Sector the "most highly regulated and heavily guarded" of all the U.S. CI sectors.[6]

A nuclear reactor presents additional challenges over fossil fuel combustion. One challenge is the generation of thermal energy when the reactor is shut down; unfortunately, the meaning of a nuclear reactor shutdown is not synonymous with "no longer producing heat." Even if the fission reaction is stopped by the reactor's shutdown mechanism, the radioactive decay of fission products continues to generate thermal energy called "decay heat" that must be removed to prevent damage to the reactor fuel. Coolant must continue to flow through the reactor core to remove this decay heat. If heat is not removed, the core could melt. This situation occurred in the Three Mile Island Unit 2 reactor in Middletown, PA in 1979 where a combination of equipment failures, design flaws, and operator error led to a meltdown of the reactor core even though the reactor was shut down.[7] The cleanup took approximately 12 years and cost $973 million.[8] The public confidence in nuclear power dropped as well.

Figure 1. Three Mile Island Nuclear Power Plant in PA[9]

SCADA System Benefits and Risks

SCADA systems can help reduce the number of personnel required to operate a power plant safely. In nuclear power plants built in the 1960s through the 1980s, SCADA systems were analog systems with hardware and software designed for a specific function, and modifying these systems was more difficult than hacking a networked component because physical access was required.[10] As these legacy systems were upgraded, programmable code usage increased the potential functions of SCADA systems, and because security was not initially designed into these systems, they have increased the vulnerability of a civilian nuclear power plant.[11]



The SCADA system reads the measured flow and level, and sends the setpoints to the PLCs

PLC1 compares the measured flow to the setpoint, controls the pump speed as required to match flow to setpoint

PLC2 compares the measured level to the setpoint, controls the flow through the valve to match level to setpoint

Figure 2. Summary of how a SCADA system with programmable logic controllers (PLC) can work[12]

Nevertheless, the problem posed by programmable code was not initially an alarming issue in systems that used SCADA components. For example, in the case of the Massachusetts Water Resource Authority, operators believed that the isolated SCADA systems were specific to a particular plant, so specialized knowledge and physical access was required to cause real damage.[13] Over time, SCADA systems have implemented open protocols and commercial off-the-shelf (COTS) software reducing the possible customization in a power plant.[14] Additionally, third parties requesting data from the nuclear power plant typically receive that data through an Internet connection, thus increasing possible avenues of attack.[15]

With 100 commercial nuclear reactors in operation at 61 power plants, there are many potential targets.[16] Each of these power plants can contain over one thousand "digital assets" which includes SCADA systems.[17] The opportunity for a cyber-attack exists through these digital assets, but according to the NEI, most of these assets are not connected to radiological safety and security.[18]

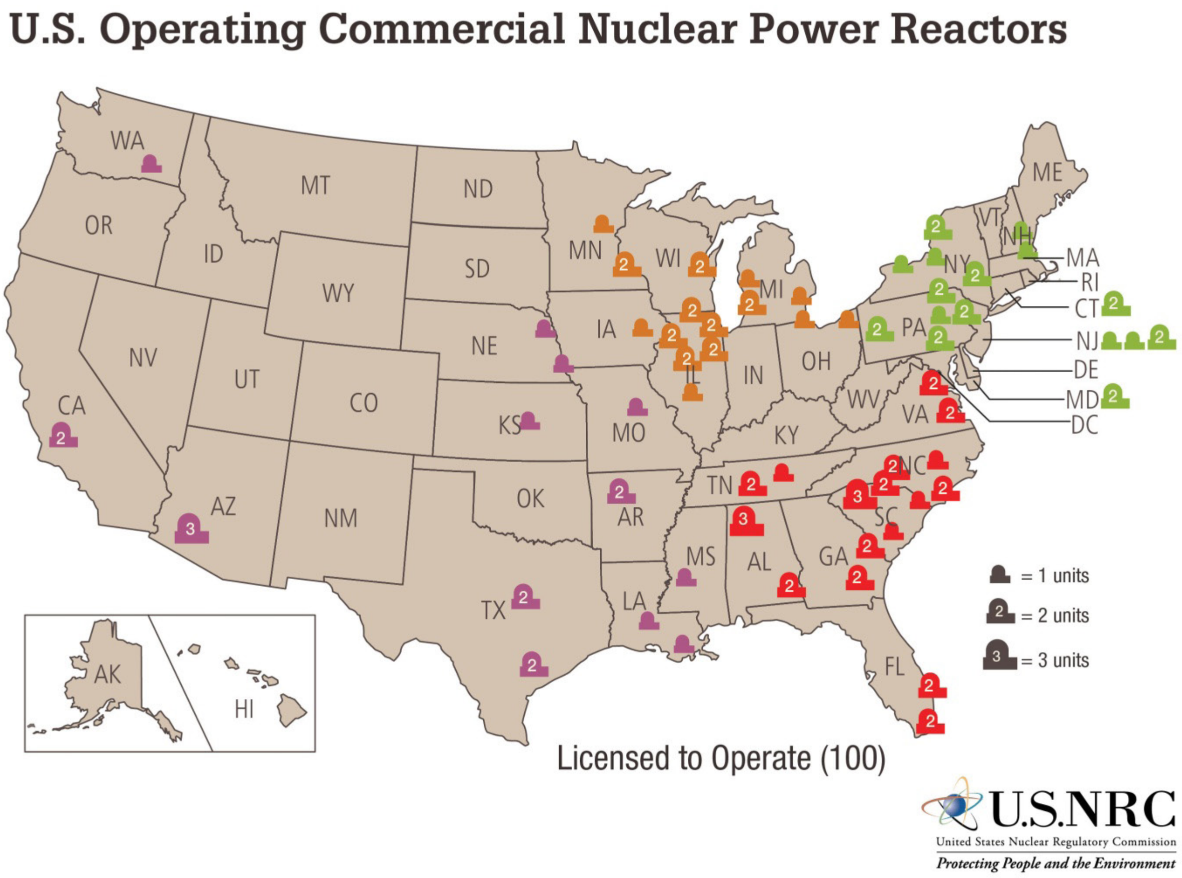

U.S. Operating Commercial Nuclear Power Reactors
WA
OR
CA
NV
ID
MT
WY
UT
AZ
CO
NM
ND
SD
NE
KS
OK
TX
MN
IA
MO
AR
LA
WI
IL
MI
IN
OH
KY
TN
MS
AL
GA
FL
SC
NC
VA
WV
PA
NY
VT
NH
ME
MA
RI
CT
NJ
DE
MD
DC
AK
HI
= 1 units
= 2 units
= 3 units
Licensed to Operate (100)
U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Figure 3. Distribution of nuclear power plants across the U.S. as of November 2015[19]

Cybersecurity Policy in Nuclear Power Plants

In the U.S., the Nuclear Regulatory Commission (NRC) is the regulatory body for all nuclear power plants.[20] Although the DHS is the sector-specific agency for the Nuclear Sector, the NRC provides oversight.[21] Thus, nuclear power plants in the U.S. have only one set of rules to follow, which helps simplify the policies and procedures required to operate a nuclear reactor.

After the terrorist attacks of September 11, 2001, the NRC directed nuclear power plant operators to improve the physical security and cybersecurity of their facilities.[22] By 2009, the NRC had codified the cybersecurity requirement in CFR Title 10, Chapter 1, Section 73.54.[23] This regulation requires an NRC-approved cybersecurity plan from current operators as well as those applying for a license to operate nuclear reactors. According to this regulation, the cybersecurity plan must protect digital systems, networks, and communications involved with

- safety,
- security,
- emergency preparedness, and
- support systems and equipment.[24]

The NRC and NEI provide additional guidance through *Regulatory Guide 5.71 Cyber Security Programs for Nuclear Facilities* and *NEI 08-09 Revision 6 Cyber Security Plan for Nuclear Power Reactors*.[25] The description of protected systems is very broad. This is likely due to the variance in design of nuclear power plants, but it forces power plant operators to analyze their own power plants to determine which digital assets would fall under safety, security, emergency preparedness, or support systems.

Nuclear Power Risk Analysis

This determination is similar to a risk analysis where assets are prioritized based on threats, vulnerabilities, and consequences if an asset is damaged or disabled.[26] Depending on their connectivity and function, SCADA systems could be classified as high risk. For example, SCADA systems involved with safety, security, or emergency preparedness likely have large consequences if they fail, and if the SCADA system is connected to the Internet through a path like a corporate network, the number of threats increases dramatically because physical access is no longer required. The trend in U.S. nuclear power plants appears to be isolation of SCADA systems connected to “critical safety and security systems.”[27]

According to the NEI, all licensed operators have cybersecurity plans that have been approved by the NRC.[28] Additionally, the NRC has approved the plan of action and milestones (POAM) for each power plant and regularly verifies the status of this POAM.[29] For example, the NRC set one milestone to occur by December 31, 2012 and it included requirements such as:

- identification of critical systems and their critical digital assets,
- isolation of critical plant systems allowing outbound communication only,
- implementation of security controls for portable media, and
- implementation of cybersecurity controls for the most important assets.[30]

Some organizations like the Chatham House, however, believe that there are fundamental flaws in both the timeliness and culture of cybersecurity protection in commercial nuclear power plants.[31] While power plants may meet the requirements set forth by the NRC, the efficacy of a cybersecurity program is measured using performance against threats, not agreement with regulations.

Cyber Threats, Vulnerabilities and Consequences

There are several cases of a commercial nuclear power plant succumbing to a cyber-attack or malfunction after 2001 that can provide a test of the cybersecurity controls in place. One example is the Slammer worm attack on the Davis-Besse Nuclear Power Station in Oak Harbor, OH in January 2003.[32] The Slammer worm infected a contractor network connected to the nuclear power station's business network which bypassed the properly configured firewall of the business network.[33] The worm then infected SCADA systems through a remote computer using a virtual private network (VPN).[34] The plant operators eventually lost the Safety Parameter Display System (SPDS) for almost five hours which required operators to walk around and manually check on plant parameters.[35] While no power outage occurred, the loss of the SPDS could slow corrective actions if a malfunction occurred within the reactor plant.

Figure 4. Davis-Besse Nuclear Power Station[36]

The Davis-Besse case highlights the vulnerability of SCADA systems when connected to the Internet. Plant operators desired to monitor plant parameters remotely and connected SCADA systems to the business network.[37] Lewis writes that the "openness and connectivity" with internal networks and external business partners is the largest security deficiency in SCADA systems.[38] The NEI shares this view, stating that the first line of defense is isolation through air gaps or hardware-based isolation.[39] However, external connections to a network can change daily, so believing that an isolated network stays isolated may be optimistic and mistaken.

Hatch Nuclear Power Plant

The Hatch nuclear power plant near Baxley, GA experienced an unexpected shutdown of one of its reactors after a software update on the business network reset data on a control network in March 2008.[40] The reactor safety program interpreted the reset as a loss of water to cool the reactor core and initiated an automatic shutdown.[41] While no damage occurred, there was a loss of electrical power generation because the plant was shut down for 48 hours.[42] The parent company, Southern Company, had to purchase electricity from another provider which cost $5 million.[43] The Hatch case shows that SCADA systems that are fed incorrect data can still take physical action based on that data; if connected to these SCADA systems, an attacker could cause a denial of service (DoS) of electrical power or worse.

Browns Ferry Nuclear Power Plant

In August 2006, the Browns Ferry nuclear reactor was shut down manually after two pumps responsible for pumping cooling water through the core failed; these pumps were controlled by variable frequency drives (VFD) which contain microprocessors that send and receive data over the control network.[44] The VFD failed due to excessive traffic on the control network, and while no damage to critical systems occurred, a loss of electrical power generation occurred similar to the Hatch power plant incident.[45] This was not due to a cyber-attack, but it shows how fragile SCADA systems can be. An attacker could execute a DoS attack by flooding the control network with useless data, and SCADA systems could fail and prevent critical components from operating, resulting in a loss of electrical power or potential reactor core damage.

Figure 5. Browns Ferry Nuclear Power Plant[46]

Recent Power Plant Hacking

In a recent wave of attacks starting in May 2017, a hacking group targeted the business networks of companies that operate nuclear power plants. One of these companies was the Wolf Creek Nuclear Operating Corporation which operates a nuclear power plant near Burlington, Kansas.[47] The DHS and FBI reported that an advanced persistent threat (APT) actor was responsible for these attacks.[48] The attackers generally attempted to exploit the insider threat by spear- phishing, or targeting specific users in order to gain sensitive information or credentials. The APT sent emails containing malicious attachments to senior engineers, hoping to steal the credentials of a recipient who opened an attachment.[49] The APT used other avenues of attack, like the watering hole attack, where a regularly-visited website is hacked to attack the users who visit, and a man-in-the-middle attack, where attackers route Internet traffic of users and their destinations through the attacker's machine.[50]

APTs differ from other attackers in that they generally focus on intelligence gathering, trade secret theft, disruption of operations, or even physical destruction of equipment; they have many financial and personnel resources, and some are backed by nation states.[51] While these attacks were aimed at the business network rather than the operational network, the information that the APT could gain from infiltrating business networks could make any future attacks on the operational network much more effective and dangerous.

The SCADA Vulnerability Market

In addition to increasing connectivity, power plants are using SCADA systems with open protocols and COTS.[52] This can allow hackers to gain knowledge about SCADA systems. An attacker can purchase a commercially available SCADA system, probe it for vulnerabilities, and use those discovered vulnerabilities against a power plant using the COTS SCADA system to gain unauthorized access. In fact, there is currently a market for this exact information, and exploits are selling at a relatively low cost.[53] For example, while Apple iOS 9 vulnerabilities can sell for up to $1 million, anonymous users can purchase SCADA vulnerabilities with an $8,100 annual subscription fee.[54] Gleg, ReVuln, and Exodus Intelligence are three companies devoted to finding SCADA vulnerabilities, and while their stance is to improve security by discovering vulnerabilities, the companies take no responsibility for what users with ill intentions may do with those exploits.[55]

Recommendations to Improve Cybersecurity

Because SCADA systems can control critical processes in a nuclear power plant, protection of these systems from cybersecurity threats is paramount. However, replacing all SCADA systems with more robust systems, known as "rip and replace," is likely infeasible due to the massive cost and downtime of critical processes required to overhaul control systems. For example, in the oil and gas sector, replacing 200 gas turbine controllers could cost up to $70 million before accounting for the cost of lost production.[56] Because nuclear equipment could be radioactive, disposal could further increase the cost of a rip and replace strategy.

Improvement of Control Networks

It may be more economically feasible for older power plants to improve the control networks on which the SCADA systems reside. Specific network improvements include redundancy, whitelisting applications, and adding an intrusion detection system (IDS) to the network.[57] Redundancy can help with patch management by shifting normal processes to one SCADA component while the other is being updated. Additionally, redundancy can assist with inadvertent activation of automated safety functions. In the case of the Hatch power plant, if two SCADA components were required to activate the safety shutdown, the plant may have avoided the shutdown. Whitelisting can help ensure that only approved applications are allowed to run on control networks that can reduce the potential effects of malware. An IDS can alert operators to abnormal conditions on the control network. In the case of the Browns Ferry shutdown, operators could have been alerted to abnormally high network traffic and mitigated the circumstances that caused the pump VFD to fail.

The conventional wisdom within the NRC, the DHS, and the NEI is that SCADA systems are protected when they are isolated or air-gapped.[58] However, critics argue that truly air-gapped systems do not exist.[59] The *Stuxnet* worm demonstrated that even air-gapped Iranian centrifuges were susceptible to infection.[60] The primary method of infection of *Stuxnet* was through USB flash drives which do not require a network connection.[61] Also, the Davis-Besse case shows that system administrators may be unaware of all connections to its SCADA control network.[62]

Minimize the Insider Threat

Another significant cybersecurity problem within commercial power plants is the insider threat.[63] The Three Mile Island accident highlighted the need for competent operators; as a result, nuclear power plant operators are typically well-trained.[64] However, this training may entrench nuclear operators in a certain way of performing their duties, and information security personnel may have difficulty trying to steer nuclear operators away from risky activities. One of these activities is connecting an operator's personal computer to the SCADA control network; this can expose the control network to any malware residing on the personal computer.[65] The attacks in 2017 demonstrate that APTs are relying on the insider threat as one way to hack into networks.

Although the operators interact directly with the control networks, supervisors and senior executives can also benefit from cybersecurity training. While those in a supervisory role are well-versed in physical security for nuclear facilities, cybersecurity is considered a low priority.[66] This could be a result of recent adoption of digital systems in nuclear power, lack of reported cybersecurity incidents at nuclear facilities, and a focus on physical security.[67]

Nuclear Power Information Sharing and Analysis Center (ISAC)

There may be a dearth of cybersecurity experts in the nuclear field, so a national organization could help provide support to nuclear supervisors. As in other CI sectors, an ISAC could be created for nuclear power plants.[68] This can be an effective way to concentrate cybersecurity expertise and provide a method for nuclear facilities to disclose anonymously cybersecurity incidents and lessons learned. The NRC could fill this role, but Kesler argues that the NRC lacks cybersecurity expertise.[69] Additionally, since the NRC functions as a regulatory body, nuclear power plants may be less likely to disclose cybersecurity incidents to the NRC than to an independent organization.

Conclusion

SCADA systems are pervasive throughout commercial nuclear power plants in the U.S. Some of these systems are involved with the safety, security, and emergency preparedness of the power plant, and licensed owners must have an NRC-approved cybersecurity plan for these systems according to 10 CFR 73.54. However, the nuclear sector may be lagging in the application of cybersecurity. Since 2001, two reported incidents involving cybersecurity resulted in a shutdown of a nuclear reactor, and one reported incident was the result of a computer worm. SCADA technology is becoming more standardized and more connected, and there is a market for their vulnerabilities, so protecting these systems is paramount. SCADA systems can be designed to be more resilient against cyber-attacks, but for older nuclear power plants that cannot feasibly rip and replace SCADA systems, improving the control network may be a more economical option. Cybersecurity training for operators and supervisors can improve security, and a nuclear ISAC could provide lessons learned from cybersecurity incidents at nuclear power plants and provide needed cybersecurity expertise to the NRC.

About the Author

Matthew Horner is a Cybersecurity Engineer with Engility Corporation in Bedford, MA assessing the risk of Air Force information systems. He was previously a Lieutenant in the US Navy and served aboard the USS Alabama, a nuclear-powered ballistic missile submarine in Bangor, WA, helping to prevent an unfriendly exchange of nuclear missiles. He may be reached at matthewshorner@gmail.com.

Notes

[1] Thomas Fox-Brewster, “Want Some Nuclear Power Plant ‘Zero Day’ Vulnerabilities? Yours for Just $8,000,” *Forbes website,* October 21, 2015.

[2] NEI, “Cybersecurity Strictly Regulated by NRC; No Additional Regulation Needed,” *NEI website,* March 2014, http://www.nei.org/CorporateSite/media/filefolder/Backgrounders/Policy-Briefs/Cyber-Security-Regulation-Strictly-Regulated-by-NRC-March-2014.pdf?ext=.pdf (accessed September 24, 2016).

[3] “Targets for Terrorism: Nuclear Power Plants,” *Council on Foreign Relations,* January 1, 2006, http://www.cfr.org/homeland-security/targets-terrorism-nuclear-facilities/p10213 (accessed October 2, 2016).

[4] The White House, *Presidential Policy Directive-21: Critical Infrastructure Security and Resilience,* Washington, DC: US Government Publishing Office, 2013.

[5] Caroline Baylon, Roger Brunt, and David Livingstone, *Cybersecurity at Civil Nuclear Facilities: Understanding the Risks,* (London: Chatham House, 2015).

[6] DHS, *Nuclear Reactors, Materials, and Waste Sector-Specific Plan,* Washington, DC: Government Printing Office, 2015.

[7] NRC, “Backgrounder on the Three Mile Island Accident,” *NRC website,* December 12, 2014, http://www.nrc.gov/reading-rm/doc-collections/fact-sheets/3mile-isle.html (accessed October 3, 2016).

[8] World Nuclear Association, “Three Mile Island Accident,” *World Nuclear Association website,* January 2012, http://www.world-nuclear.org/information-library/safety-and-security/safety-of-plants/three-mile-island-accident.aspx (accessed October 8, 2016).

[9] US Department of Energy, *March 28, 1979: Three Mile Island,* https://energy.gov/management/march-28-1979-three-mile-island (accessed December 7, 2016).

[10] Caroline Baylon, Roger Brunt, and David Livingstone, *Cybersecurity at Civil Nuclear Facilities: Understanding the Risks,* (London: Chatham House, 2015).

[11] Ibid.

[12] *SCADA Schematic Overview,* September 18, 2013, https://commons.wikimedia.org/wiki/File:SCADA_schematic_overview-s.svg (accessed December 7, 2016).

[13] Scott Berinato, “Debunking the Threat to Water Utilities,” *CIO Magazine website,* March 15, 2002, http://www.cio.com/article/2440931/security0/debunking-the-threat-to-water-utilities.html (accessed October 3, 2016).

[14] Brent Kesler, “The Vulnerability of Nuclear Facilities to Cyber Attack,” *Strategic Insights* 10, no. 1 (2011): 15-25.

[15] Caroline Baylon, Roger Brunt, and David Livingstone, *Cybersecurity at Civil Nuclear Facilities: Understanding the Risks,* (London: Chatham House, 2015).

[16] NRC, *Map of Power Reactor Sites,* November 13, 2015, http://www.nrc.gov/reactors/operating/map-power-reactors.html (accessed December 7, 2016).

[17] Jessie Smith, “Cybersecurity is Alive and Well in US Nuclear Power Plants,” *National Cybersecurity Institute website,* December 10, 2015, http://www.nationalcybersecurityinstitute.org/energy-utilities/cybersecurity-is-alive-and-well-in-us-nuclear-power-plants/ (accessed October 3, 2016).

[18] NEI, “Cyber Security for Nuclear Power Plants,” *NEI website,* July 2016, http://www.nei.org/Master-Document-Folder/Backgrounders/Policy-Briefs/Cyber-Security-for-Nuclear-Power-Plants (accessed October 3, 2016).

19 NRC, *Map of Power Reactor Sites,* November 13, 2015, http://www.nrc.gov/reactors/operating/map-power-reactors.html (accessed December 5, 2016).

20 US Government, "CFR Title 10 Chapter 1," *GPO website*, 2016, https://www.gpo.gov/fdsys/browse/collectionCfr.action?collectionCode=CFR&searchPath=Title+10&oldPath=&isCollapsed=true&selectedYearFrom=2016&ycord=285.

21 The White House, *Presidential Policy Directive-21: Critical Infrastructure Security and Resilience*, Washington, DC: US Government Publishing Office, 2013; NEI, "Cybersecurity Strictly Regulated by NRC; No Additional Regulation Needed," *NEI website*, March 2014, http://www.nei.org/CorporateSite/media/filefolder/Backgrounders/Policy-Briefs/Cyber-Security-Regulation-Strictly-Regulated-by-NRC-March-2014.pdf?ext=.pdf (accessed September 24, 2016).

22 NEI, "Cyber Security for Nuclear Power Plants," *NEI website,* July 2016, http://www.nei.org/Master-Document-Folder/Backgrounders/Policy-Briefs/Cyber-Security-for-Nuclear-Power-Plants (accessed October 3, 2016).

23 NRC, "10 CFR 73.54 Protection of Digital Computer and Communication Systems and Networks," *NRC website,* December 2, 2015, http://www.nrc.gov/reading-rm/doc-collections/cfr/part073/part073-0054.html (accessed September 24, 2016).

24 Ibid.

25 NRC, "Regulatory Guide 5.71 Cyber Security Programs for Nuclear Facilities," *NRC website,* January 2010, http://www.nrc.gov/docs/ML0903/ML090340159.pdf (accessed October 5, 2016); NEI, "NEI 08-09 Rev 6 Cyber Security Plan for Nuclear Power Reactors," *NRC website,* April 2010. http://www.nrc.gov/docs/ML1011/ML101180437.pdf (accessed October 5, 2016).

26 NIST, "NIST SP 800-30 Revision 1 Guide for Conducting Risk Assessments," *NIST website,* September 2012, http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf (accessed October 4, 2016).

27 NEI, "Cyber Security for Nuclear Power Plants," *NEI website,* July 2016, http://www.nei.org/Master-Document-Folder/Backgrounders/Policy-Briefs/Cyber-Security-for-Nuclear-Power-Plants (accessed October 3, 2016).

28 NEI, "Cybersecurity Strictly Regulated by NRC; No Additional Regulation Needed," *NEI website,* March 2014, http://www.nei.org/CorporateSite/media/filefolder/Backgrounders/Policy-Briefs/Cyber-Security-Regulation-Strictly-Regulated-by-NRC-March-2014.pdf?ext=.pdf (accessed September 24, 2016).

29 Ibid.

30 Jessie Smith, "Cybersecurity is Alive and Well in U.S. Nuclear Power Plants," *National Cybersecurity Institute website,* December 10, 2015, http://www.nationalcybersecurityinstitute.org/energy-utilities/cybersecurity-is-alive-and-well-in-us-nuclear-power-plants/ (accessed October 3, 2016).

31 Caroline Baylon, Roger Brunt, and David Livingstone, *Cybersecurity at Civil Nuclear Facilities: Understanding the Risks,* (London: Chatham House, 2015).

32 Michel Kabay, "Attacks on Power Systems: Hackers, Malware," *Network World website,* September 13, 2010, http://www.networkworld.com/article/2217684/data-center/attacks-on-power-systems--hackers--malware.html (accessed October 7, 2016).

33 Ibid.

34 Ibid.

35 Brent Kesler, "The Vulnerability of Nuclear Facilities to Cyber Attack," *Strategic Insights* 10, no. 1 (2011): 15-25.

36 NRC, *Davis-Besse Nuclear Power Station, Unit 1,* February 10, 2017, https://www.nrc.gov/info-finder/reactors/davi.html (accessed February 15, 2017).

37 Brent Kesler, “The Vulnerability of Nuclear Facilities to Cyber Attack,” *Strategic Insights* 10, no. 1 (2011): 15-25.

38 Ted Lewis, *Critical Infrastructure Protection in Homeland Security,* 2nd. (Hoboken, NJ: John Wiley & Sons, Inc, 2015).

39 NEI, “Cyber Security for Nuclear Power Plants,” *NEI website,* July 2016, http://www.nei.org/Master-Document-Folder/Backgrounders/Policy-Briefs/Cyber-Security-for-Nuclear-Power-Plants (accessed October 3, 2016).

40 Brent Kesler, “The Vulnerability of Nuclear Facilities to Cyber Attack,” *Strategic Insights* 10, no. 1 (2011): 15-25.

41 Caroline Baylon, Roger Brunt, and David Livingstone, *Cybersecurity at Civil Nuclear Facilities: Understanding the Risks,* (London: Chatham House, 2015).

42 Ibid.

43 Terry Hardy, *Software and System Safety,* AuthorHouse, 2012.

44 Brent Kesler, “The Vulnerability of Nuclear Facilities to Cyber Attack,” *Strategic Insights* 10, no. 1 (2011): 15-25.

45 Ibid.

46 US Tennessee Valley Authority, TVA.gov, https://www.tva.gov/file_source/TVA/Site%20Content/Energy/Our%20Power%20System/Nuclear/Images/Browns-Ferry.jpg (accessed February 15, 2017).

47 Nicole Perlroth, “Hackers Are Targeting Nuclear Facilities, Homeland Security Dept. and F.B.I. Say,” *The New York Times website,* July 6, 2017. https://www.nytimes.com/2017/07/06/technology/nuclear-plant-hack-report.html. (accessed January 18, 2018).

48 Ibid.

49 Ibid.

50 Ibid.

51 Symantec, “Advanced Persistent Threats: A Symantec Perspective,” *Symantec Corporation website,* November, 2011, https://www.symantec.com/content/en/us/enterprise/white_papers/b-advanced_persistent_threats_WP_21215957.en-us.pdf. January 18, 2018.

52 Brent Kesler, “The Vulnerability of Nuclear Facilities to Cyber Attack,” *Strategic Insights* 10, no. 1 (2011): 15-25.

53 Thomas Fox-Brewster, “Want Some Nuclear Power Plant ‘Zero Day’ Vulnerabilities? Yours for Just $8,000,” *Forbes website,* October 21, 2015.

54 Ibid.

55 Ibid.

56 Eric Byres, “Enough Clucking - Start Fixing the SCADA Security Problem,” *Tofino Security website,* September 9, 2013, https://www.tofinosecurity.com/blog/enough-clucking-%E2%80%93-start-fixing-scada-security-problem (accessed October 8, 2016).

57 Caroline Baylon, Roger Brunt, and David Livingstone, *Cybersecurity at Civil Nuclear Facilities: Understanding the Risks,* (London: Chatham House, 2015).

58 NRC, "Regulatory Guide 5.71 Cyber Security Programs for Nuclear Facilities," *NRC website,* January 2010, http://www.nrc.gov/docs/ML0903/ML090340159.pdf (accessed October 5, 2016); DHS, *Nuclear Reactors, Materials, and Waste Sector-Specific Plan,* Washington, DC: Government Printing Office, 2015; NEI, "Cyber Security for Nuclear Power Plants," *NEI website,* July 2016. http://www.nei.org/Master-Document-Folder/Backgrounders/Policy-Briefs/Cyber-Security-for-Nuclear-Power-Plants (accessed October 3, 2016).

59 Brent Kesler, "The Vulnerability of Nuclear Facilities to Cyber Attack," *Strategic Insights* 10, no. 1 (2011): 15-25; Caroline Baylon, Roger Brunt, and David Livingstone, *Cybersecurity at Civil Nuclear Facilities: Understanding the Risks,* (London: Chatham House, 2015).

60 Kim Zetter, "An Unprecedented Look at Stuxnet, The World's First Digital Weapon," *Wired website,* November 3, 2014, https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/ (accessed September 24, 2016).

61 Ibid.

62 Brent Kesler, "The Vulnerability of Nuclear Facilities to Cyber Attack," *Strategic Insights* 10, no. 1 (2011): 15-25.

63 Caroline Baylon, Roger Brunt, and David Livingstone, *Cybersecurity at Civil Nuclear Facilities: Understanding the Risks,* (London: Chatham House, 2015).

64 World Nuclear Association, "Three Mile Island Accident," *World Nuclear Association website,* January 2012, http://www.world-nuclear.org/information-library/safety-and-security/safety-of-plants/three-mile-island-accident.aspx (accessed October 8, 2016).

65 Caroline Baylon, Roger Brunt, and David Livingstone, *Cybersecurity at Civil Nuclear Facilities: Understanding the Risks,* (London: Chatham House, 2015).

66 Ibid.

67 Ibid.

68 Ted Lewis, *Critical Infrastructure Protection in Homeland Security,* 2nd. (Hoboken, NJ: John Wiley & Sons, Inc, 2015).

69 Brent Kesler, "The Vulnerability of Nuclear Facilities to Cyber Attack," *Strategic Insights* 10, no. 1 (2011): 15-25.