Outpacing Cyber Threats: Priorities for Cyber Security at Nuclear Facilities

A. Van Dine[1], M. Assante[2], P. Stoutland [1]

[1]Nuclear Threat Initiative, Washington, D.C., United States of America

[2]SANS Institute, Bethesda, MD, United States of America

E-mail contact of main author: vandine@nti.org

Abstract

Ensuring the security of nuclear facilities is a critical element in preventing theft of nuclear materials and sabotage that could result in a radiological release. While the international community has traditionally focused on improving physical security to prevent these outcomes by investing in the "guns, guards, and gates" trifecta, a newer threat has gained attention: the cyber threat. A cyber-attack perpetrated by a terrorist group on a nuclear facility could have physical consequences leading to either an act of theft or sabotage. This threat presents new challenges to facility operators as well as national authorities. Given the increasing reliance upon digital controls, it is expected that these challenges will only continue to grow.

A security lapse at a nuclear facility leading to theft of nuclear material or a catastrophic radiological release would have global implications—an incident anywhere would have consequences everywhere, and would cast doubt on industry-wide security practices. Therefore, all countries must have effective cybersecurity measures in place. Currently, government authorities and facility operators are struggling to keep pace with this new threat, battling issues such as high costs, bureaucratic inertia, highly complex systems, cultures of compliance, and a shortage of demonstrably qualified personnel. National and international guidance has evolved over the past year, but not quickly enough to address the growing gap between attacker and defender capabilities in cyberspace.

Recognizing that the growing sophistication of cyber threats increasingly taxes the capabilities of governments, national regulators, and facility operators around the world, the Nuclear Threat Initiative (NTI) has concluded that a fresh look at the overarching framework that guides cybersecurity implementation at nuclear facilities is an urgent, necessary precursor to achieving essential progress in this area. Despite valuable ongoing efforts at the national and international level, more must be done. A more effective and perhaps disruptive approach, based on a set of high-level priorities, is critical to getting ahead of this threat.

Over the past year, NTI has engaged in conversation with experts and undertaken research to identify and further develop high-level priorities to guide the implementation of cybersecurity at nuclear facilities. Such a framework would be a crucial first step in shaping an international, ambitious, forward-looking global strategy in this area. This paper defines the fundamental priorities that make up this framework while situating them in a broader context of the cyber threat to nuclear facilities and the challenges faced by national authorities and facility operators.

Key Words: cyber security, nuclear safety, nuclear security, nuclear facilities

1. Introduction

The past decade has seen unprecedented progress in the security of nuclear materials and facilities. As key improvements to physical security have been implemented, however, a potentially more dangerous threat is undermining these gains: the cyber threat.

Cyber-attacks could be used to facilitate the theft of nuclear materials or an act of sabotage resulting in radiological release. A successful attack could have consequences that

reverberate around the world and undermine global confidence in civilian nuclear power as a safe and reliable energy source. Given the risk and the stakes, governments and industry must now increase focus on the cyber threat.

Nuclear operators and a range of national and international organizations have recognized the challenge and have begun to accelerate their efforts to strengthen cyber security at nuclear facilities. However, the rapidly evolving cyber threat, combined with the proliferation of digital systems, makes it difficult to get ahead of the threat. Case after case—from the Stuxnet attacks on the Natanz uranium enrichment facility in Iran, to the hack of Korea Hydro and Nuclear Power in South Korea, to disturbing revelations of malware seeking login credentials found on systems at a German nuclear power plant—demonstrates that the current approach to cyber security at nuclear facilities is falling short, and will soon be insufficient. Crafting a strategy that protects facilities from the dynamic, evolving cyber threats they now face requires a fresh, unconstrained examination of the overarching framework that guides their cyber security.

To get ahead of this threat, the Nuclear Threat Initiative (NTI) assembled an international group of technical and operational experts with backgrounds in computer security, nuclear safety systems, nuclear engineering, industrial control systems, and nuclear facility operations. This group was tasked with identifying the core elements of a new strategy, then focusing on those elements that would have the greatest possible impact.

Over 12 months, the group identified four overarching priorities that, if implemented, would dramatically reduce the risk of damaging cyber-attacks on nuclear facilities. Although similar concepts are in use elsewhere, alone and in combination, each of these priorities would provide unique leverage on the threat posed to nuclear facilities.

These priorities are: **institutionalize cyber security**, **mount an active defense**, **reduce complexity**, and **pursue transformation**; they are outlined in greater detail later in this paper.

This paper is based on an official NTI report recommending several near-term actions that governments, regulators, and international organizations can and should take now to begin implementing a new strategy based on the above priorities. Taken together, these priorities represent a new approach to getting ahead of the urgent and evolving cyber threat. Implementing them will be a multi-year effort and it will not be easy, but the risk is far too great to remain on the current path.

2. Threat

Today, both safety and physical protection systems rely on digital components that could be compromised by a determined adversary. For example, researchers have shown that a cyber-attack could be used to disable physical protection measures like closed-circuit television cameras to allow an intruder unfettered access to sensitive areas of a facility. [1] Additionally, an attacker could manipulate nuclear reactor control systems; this could potentially lead to events causing a radiological release. Finally, the threat is not only from outsiders—damaging actions could be taken with the assistance of an insider, whether wittingly or unwittingly. [2]

Recent history is filled with examples demonstrating that critical infrastructure and even nuclear facilities are vulnerable—both to untargeted malware and targeted cyber-attacks. As is now well known, the Natanz uranium enrichment facility in Iran was attacked with the Stuxnet virus between 2009 and 2010, damaging centrifuges and delaying enrichment activities. [3] This case is particularly notable as the facility was described as well-defended and isolated from the internet.

Since news of Stuxnet broke, revelations of malware found in nuclear facilities and critical infrastructure have only increased in frequency. In 2014 alone, a cyber-attack against a German steel mill caused massive physical damage, malware was introduced into the control room at Japan's Monju nuclear power plant, and systems associated with the Korea Hydro and Nuclear Power in South Korea was hacked. The Japanese and South Korean cases resulted in the release of technical data online. [4] [5] [6] The year 2015 saw a sophisticated, troubling cyber-attack—one that it is not hard to imagine being used against a nuclear facility—against the Ukrainian power grid that turned out the lights in portions of that country for between three and six hours. [7] [8] And in 2016, a German nuclear power plant , and a Japanese facility that handles plutonium and other nuclear materials revealed that they had discovered malware in its systems. [9] [10].

It may only be a matter of time before the world experiences a catastrophic event—whether a theft of nuclear material, or the sabotage of a nuclear facility—facilitated by a cyber-attack deployed by a determined, well-resourced adversary. Those responsible for security, from policymakers to regulators to industry leaders to facility operators, face the significant challenge of getting ahead of the fast-moving threat.

3. Current Status and Approach

Digital systems are integral to nuclear facilities throughout the fuel cycle, from enrichment facilities to reprocessing plants to spent fuel storage to nuclear power plants, and they perform a range of functions, including access control, materials control and accounting, and the safe and secure operation of the facility.

To date, the approach for managing cyber risks has focused on preventing access to critical systems using tools such as firewalls, antivirus programs, air gaps, and unidirectional gateways.[1] This approach has generally proven effective against untargeted cyber-attacks—the cyber threat that has plagued computer users for the last decade—but it is not sufficient to protect against newer, target-focused attacks and threats. These tend to rely upon more enduring vulnerabilities, such as human behaviors and practices, and may include creating new cyber weapons.[2]

[1] Unidirectional security gateways are replacing the overly restrictive air-gap in the forms of data diode technologies.

[2] The ability to exploit weaknesses in the complex system-of-systems that comprise modern organizations has invented underground markets, empowered activists, and transformed intelligence gathering and war fighting. Many enterprises have mastered the art and science of maneuvering through the expected noise and less structured threats that come with global public networks. The adversarial "cyber" threat actors that engage in targeted attacks continue to expand at an alarming rate, defeating security prevention and detection technology/controls, challenging conventional analysis, and invalidating existing reliability and safety design methods. Examples include campaigns and malware such as Snake, Ice Fog, Black Energy, Duqu, MiniDuke, Stuxnet, Regin, Night Dragon, etc.

In contrast to unsophisticated attackers, determined adversaries are known to use targeted, adaptive strategies and customized cyber tools and may even consider compromising the supply chain. In practice, targeted attacks have proven effective in overcome conventional cyber security defenses, and it is evident that well-resourced, persistent adversaries can defeat [11] even technologically advanced security solutions. [12] The weapons used in these attacks upend the traditional assumption that malware infections on facility systems are benign, as they cannot communicate out from the network. As attacks like Stuxnet have shown, attackers may only need to deliver autonomous malware capable of making its own decisions.

In the context of nuclear facilities, it is also important to not just recognize the potential consequences of what digital systems are designed to do but also what they are *capable* of doing. System engineers often think in terms of what the system is *designed* to do, but adversaries tend to think in terms of what they system can be *made* to do. As this is only beginning to be realized, many of the potential outcomes of a cyber-attack on a nuclear facility have yet to be analyzed.

Protecting nuclear facilities from damaging cyber-attacks is made more difficult by their complexity. A typical facility might include more than a thousand digital components, including legacy systems with no built-in security. In addition, older facilities are transitioning to digital systems that while often bringing greater reliability and safety, also become more vulnerable to cyber-attacks. In addition to making defense more difficult, complexity increases attack pathways, including the creation of unanalyzed failure modes that would never occur naturally.

Finally, getting ahead of the cyber threat is exacerbated by a shortage of technical expertise in the cyber-nuclear space. Finding experts with specific knowledge of digital control systems in a nuclear environment is no easy feat. What expertise does exist tends to be overwhelmingly concentrated in North America, Europe, and Russia—leaving many countries with new or expanding nuclear energy programs grasping for solutions.

Current Approach

Nuclear operators and a range of national and international organizations have recognized the challenge and begun to accelerate their efforts to strengthen cyber security at nuclear facilities. For example, in the United States, the Nuclear Regulatory Commission (NRC) and the Department of Homeland Security (DHS) have clearly defined roles in protecting nuclear facilities from cyber-attacks. At the international level, important efforts have been undertaken by the International Atomic Energy Agency (IAEA) and the World Institute for Nuclear Security (WINS). The IAEA, for example, provides hands-on training in cyber security at nuclear facilities to member states, and has worked to develop and publish guidance for developing and implementing cyber security plans at nuclear facilities.[3] [13] [14] [15] Finally, the importance of cyber security at nuclear facilities was highlighted at the 2016 Nuclear Security Summit and the Nuclear Industry Summit.

[3] The IAEA has published at least three relevant documents and is continuing to work hard to assemble guidance on this issue. Please see references for more information.

This paper approaches the problem differently than existing efforts. NTI's efforts to develop priorities for cyber security at nuclear facilities have focused on the root causes of vulnerabilities. Although guidance for treating the symptoms of the cyber threat is valuable, getting ahead of the threat is impossible without addressing *why* facilities are vulnerable.

4. Developing Priorities for Action

In response to current realities and challenges, NTI assembled an international group of technical and operational experts with backgrounds in computer security, nuclear safety systems, nuclear engineering, industrial control systems, and nuclear facility operations. This group was tasked with identifying the core elements of a new strategy, focusing on those elements that would have the greatest possible impact.

Over 12 months, the group identified four priorities that, if implemented, would dramatically reduce the risk of damaging cyber-attacks on nuclear facilities. In many ways these priorities are not novel—similar concepts are in use elsewhere. Alone and in combination, however, each would provide unique leverage on the threat posed to nuclear facilities. These priorities are detailed below:

Priority: Institutionalize Cyber Security

Since the partial nuclear reactor meltdown at Three Mile Island in 1979, and more recently the terrorist attacks of September 11, 2001, nuclear facilities have focused much of their attention on preventing accidents and physical security lapses. Today, these safety and security programs are largely institutionalized and part of daily operations, and address plant design and choice of technologies, hiring, management and training of the people hired to work at a facility, and processes to govern operations.

Although safety and security are generally considered as separate concerns, the increasingly widespread use of digital technologies at nuclear facilities has virtually eliminated the gap between them. Recognizing that cyber-attacks may have serious physical consequences on par with a safety or security incident, cyber security must be treated with at least the same rigor and attention as safety and physical security. Specifically, cyber security must be embedded in the daily operations of a nuclear facility in three key areas:

- **People and organizational culture**: Where cyber security is concerned, human vulnerabilities are enduring and must be addressed. Lessons learned from both safety and physical security illustrate the importance of personnel understanding their role and how it fits into a larger context. As such, awareness of the importance of cyber security should be embedded throughout the organization, from the CEO to the most junior employees, and reinforced in personnel hiring, interaction, and assessment.

- **Design solutions**: Systems at nuclear facilities must be designed and defended appropriately. Lessons learned from the graded application of safety and physical security measures can be applied to cyber security to ensure that the systems performing the most important functions are engineered to be the least likely to fail. Under this graded approach, options for designing the most critical systems would be significantly constrained and subject to more stringent requirements—from design, to procurement, to implementation— to minimize the likelihood of failure.

- **Facility processes and practices**: Effective processes and practices are essential for the safe and secure operation of nuclear facilities and as such, must ensure that digital systems are designed, operated and maintained appropriately in the face of the cyber threat. Practices should include classifying digital systems, outlining permissible system architectures, defining change and review processes, and updating procedures for response to severe incidents.

Implementation of robust processes and practices is essential for the effective management of complex systems and is at the heart of long-standing quality management programs implemented across industry. Given the rapidly evolving cyber threat, however, this is generally not yet the case for cyber security in nuclear facilities. Nuclear facilities should learn from and actively integrate the practices employed by safety and physical security programs to strengthen and sustain their cyber security programs.

Priority: Mount an Active Defense:

As digital technologies have spread, cyber vulnerabilities have grown—often, without the full awareness of those tasked with defending the systems. Cyber defense strategies at nuclear facilities tend to rely on the concept of static prevention. Unfortunately, this approach may be insufficient.[4] Cases mentioned earlier demonstrate that commonly relied-upon measures like air gaps, firewalls, and antivirus programs fail against even untargeted viruses and likely would crumble in the face of a well-resourced, determined adversary.

An effective "active defense" capability is essential to developing stronger cyber defenses. For the purposes of this report, *active defense is defined as the continuous process of analysts monitoring for, responding to, learning from, and applying their knowledge of threats internal to the network in order to detect, block, and expel adversaries*.[5] Such a strategy incorporates the lessons learned from recent attacks on critical infrastructure and assumes that it is not possible to prevent all cyber-attacks before they occur. The ultimate goal is to develop and implement a capability that allows facility staff to detect and disrupt cyber intrusions and attackers as they happen—a pragmatic approach to cyber defense.

Implementation will require several steps. Facilities would need to characterize their systems and conduct risk analyses and engineering evaluations to determine which systems and data are most important and vulnerable. Armed with an understanding of which systems are most critical and how systems function and interact, the cyber security team can focus on detecting attackers, anticipating their next moves, and eliminating their attack opportunities.

This mission requires a team with a variety of skill sets, including threat intelligence analysts, intrusion analysts, incident responders, forensic analysts, and malware reverse engineers, and team directors. Team members could be present either on- or off-site. A key challenge will be difficulties associated with hiring and retaining highly technical staff; one solution could be for national governments to make experts available or to develop shared technical resources. Today's static cyber security architectures at nuclear facilities are not effective enough on their own to prevent a breach by a determined adversary, nor are they effective enough to

[4] For example, the Stuxnet virus infected a highly sensitive uranium enrichment facility that was air-gapped.
[5] In other industries, the term "active defense" can sometimes carry the connotation that defenders should "hack back" against adversaries. The term is used here merely to indicate a dynamic defense, distinct from "hacking back." The authors do not advocate the "hack back" approach.

respond once a compromise has occurred. Nuclear facilities need to update their prevention and response plans, steps that are essential, yet challenged by the global shortage of technical experts.

Priority: Reduce Complexity:

While digitization has brought many benefits, the accompanying complexity (of systems and environments alike) compromises cyber security in two key ways. First, it heightens the likelihood that various components have unknown functionalities or interactions that can serve as an entry point for an adversary. Second, it leads to higher levels of activity and "noise" on the network, which can camouflage an adversary's movements.

Systems at nuclear facilities can be built on top of one another over time are too often not fully understood by any one individual or operational entity. Thousands of nodes communicate across multiple layers in a variety of protocols, operating systems, and shared applications. Technologies offered by vendors often include a variety of modes of connectivity, ranging from non-declared radio communications devices to Bluetooth and Wi-Fi. [16] Moreover, generic system designs that are in use in facilities around the world can include intricate layers of enhanced features and functionalities that are very difficult to understand—especially when crafted without security as a primary consideration.

In addition, regulators, vendors, and operators face a significant challenge in the supply chain from which all facility technologies are sourced. Vendors in the supply chain are not held accountable for the security of the products and services they provide—and in many cases, would not even be capable of assuring security. [17] Because each stage of information exchange—from design to delivery—provides a new opportunity for exploitation, the supply chain exacerbates the complexity conundrum and can even introduce new and undetected cyber vulnerabilities to nuclear facilities.

System complexity also has made defense more challenging, but regulators and operators alike have continued to use outdated physical security models for threat, response, and deterrence in cyberspace and rely on compliance-based regulations to address the cyber threat. Unfortunately, this strategy can only manage the cyber threat—not eliminate it.

Complexity is the enemy of security. To best defend systems, facility operators should work to reduce complexity wherever possible in systems controlling critical functions of nuclear processes. Where complexity must exist, it should be appropriately documented and commensurate with the level required to accomplish only the system's immediate task. Those systems performing the most important functions should be engineered to be the least likely to fail. In some cases, recognizing the trade-offs, it may be appropriate to transition to non-digital systems to greatly reduce the cyber threat.

Priority: Pursue Transformation

The global community is in the early stages of understanding the magnitude of the cyber threat. In many ways, humans have created systems that are too complex to manage—in most cases, risks cannot even be fully quantified. As a result, there is a fundamental need for transformative research to develop hard-to-hack systems for critical applications.

While the priorities outlined in this paper thus far constitute pillars of a more robust strategy, in the long term, getting ahead of the growing threat will require new approaches, methods, and technologies. This is particularly true for cyber-physical systems, including nuclear facilities, in which safety and security are intertwined. While development of high-assurance and resilient systems is becoming an increasingly active area of research, much more is needed—especially in the nuclear space.[6] [18] [19]

Building robust and secure systems (i.e., trustworthy and defendable systems) for critical applications will require rigorous software and hardware development, as well as means to assess and verify the trustworthiness and security. As an example, research is underway currently on the application of formal methods [20] to ensure that software and hardware is functionally correct and also meets the safety and security goals. This approach is already used for critical NASA applications and automated train safety systems and is being improved through existing R&D programs [21], but it must be developed and applied more broadly for critical applications.

In addition to hardening the hardware and software, improved models are needed to simulate the behavior of these complex cyber-physical systems and to understand the potential implications of a cyber-attack. When developed, such models could provide a basis for cyber-induced safety analysis as existing risk models are not applicable. Models exist to simulate the behavior of safety-related failures; they are typically unable to consider multiple operations, failures or widespread loss of data integrity that would never occur naturally but could be induced via a concerted cyberattack.

Research also should pursue the development of *21st century non-digital solutions* that would be inherently secure. Yesterday's analog technologies were not as vulnerable to cyberattacks, and many nuclear facilities continue to benefit from these systems. As these systems become obsolete, they are being replaced with digital systems with increased performance and reliability, but also with cyber vulnerabilities. It may be possible, however, to develop new, non-digital approaches that are cyber-secure and have the improved performance characteristics necessary. For example, a solid-state analog solution [22] was recently announced to eliminate vulnerability to Aurora-type attacks. [23] Other potential areas for research and development include high-integrity communication channels for cyber defenders to use, as well as methods and models for going beyond traditional cyber detection to identify attacker experimentations or actions. In the future, one can envision using modern technologies to construct high-performance, verifiable, non-digital solutions for critical safety and security functions.

5. Taking Action

Countries have made great strides in improving physical security at nuclear facilities in the last several years in the name of preventing a catastrophic act of nuclear terrorism. Many of the same outcomes can be achieved in the cyber realm—making it more important than ever to pursue an ambitious, forward-looking strategy grounded in technically-sound priorities for improving cyber security at nuclear facilities. Recognizing that an investment of time, focus,

[6] For example, within the U.S. DoD, DARPA has a research programs to develop High-Assurance Cyber Military Systems (HACMS). See references for more information and examples.

and resources will be required, there are certain actions that governments, regulators, industry, and international organizations can and should take now to begin the process of implementing a new strategy based on the above priorities. Specifically:

- Governments and regulators should integrate these priorities into national policies and requirements in several ways, including prioritizing the development of regulatory frameworks, supporting—with financial, personnel, and research resources—efforts to minimize complexity in critical facility systems and re-tool facility defense strategies, and investing in augmenting human capacity, research, and development in the cyber-nuclear space.

- The nuclear industry and nuclear facilities should work together to apply lessons learned from institutionalizing safety and physical security to cyber security, develop cross-industry defense resources, demand more secure, less complex products from vendors, and work to recruit the expertise necessary to achieve a more secure future.

- International organizations should support and encourage a renewed focus on cyber security at nuclear facilities, continue to think creatively about how to get ahead of this threat and recruit a variety of voices and perspectives to contribute, and facilitate key research and development.

Taken together, the priorities above represent a new approach to getting ahead of this evolving threat.

6. Conclusion

Cyber threats bridge the gap between nuclear safety and security risks, and pose a serious challenge to global progress on nuclear security. A cyberattack could be used to cause a safety event, such as a radiological release, or a security breach, such as the theft of nuclear materials. The consequences of such an attack would be global in scope, and ongoing efforts to address this threat, while valuable, have been unable to keep pace. A new strategy, based on technically sound and forward-looking strategic priorities is necessary to get ahead of this threat.

Institutionalizing cyber security at nuclear facilities, implementing active defense strategies and minimizing complexity would address many of the serious vulnerabilities the world faces today. Investing in transformative research and development will lay the groundwork for an even more secure future.

Governments and industry each have a role to play in addressing and outpacing this threat. The risk is too great to preserve the status quo.

References

[1] QUEVENCO, R., “Secure Computer Systems Essential to Nuclear Security, Conference Finds,” IAEA Office of Public Information and Communication (2015), https://www.iaea.org/newscenter/news/secure-computer-systems-essential-nuclear-security-conference-finds

[2] SAMANI, R., AND MCFARLAND, C., “Hacking the Human Operating System: The Role of Social Engineering Within Cybersecurity," McAfee Incorporated (2015), http://www.mcafee.com/de/resources/reports/rp-hacking-human-os.pdf

[3] WARRICK, J. “Iran's Natanz nuclear facility recovered quickly from Stuxnet cyberattack,” Washington Post Foreign Service (2011), http://www.washingtonpost.com/wp-dyn/content/article/2011/02/15/AR2011021505395.html

[4] ZETTER, K., “A cyberattack has cause confirmed physical damage for the second time ever,” Wired (2015), https://www.wired.com/2015/01/german-steel-mill-hack-destruction/

[5] PAGANINI, P. “IT administrator at Monju Nuclear Power Plant discovered that a malware-based attack infected a system in the reactor control room,” Security Affairs (2014), http://securityaffairs.co/wordpress/21109/malware/malware-based-attack-hit-japanese-monju-nuclear-power-plant.html

[6] CHO, M. and KIM, J., “South Korea nuclear plant operator says hacked, raising alarm,” Reuters (2014), http://www.reuters.com/article/us-southkorea-nuclear-idUSKBN0K008E20141222

[7] ZETTER, K., “Inside the cunning, unprecedented hack of Ukraine's power grid,” Wired (2016), https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/

[8] ASSANTE, M.J. and LEE, R.M., “Analysis of the Cyber Attack on the Ukrainian Power Grid: Defense Use Case,” Electricity Information Sharing and Analysis Center (2016), http://www.nerc.com/pa/CI/ESISAC/Documents/E-ISAC_SANS_Ukraine_DUC_18Mar2016.pdf

[9] “German nuclear plant suffers cyber attack designed to give hackers remote access,” The Telegraph (2016), http://www.telegraph.co.uk/news/2016/04/27/cyber-attackers-hack-german-nuclear-plant/

[10] “Nuclear center waits over a year to report cyber-attack,” The Asahi Shimbun (2016), http://www.asahi.com/ajw/articles/AJ201605190028.html

[11] O'REGAN, R., “3 of the Biggest Concerns About External Cyber Threats,” Art of the Hack (2016), http://theartofthehack.com/3-of-the-biggest-concerns-about-external-cyber-threats/

[12] RAGAN, S., “Researcher discloses zero-day vulnerability in FireEye,” CSO Online, (2015), http://www.csoonline.com/article/2980937/vulnerabilities/researcher-discloses-zero-day-vulnerability-in- fireeye.html

[13] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Series No. 17 Technical Guidance Reference Manual: Computer Security at Nuclear Facilities, Vienna (2011).

[14] INTERNATIONAL ATOMIC ENERGY AGENCY, Specific Safety Guide No. SSG-39: Design of Instrumentation and Control Systems for Nuclear Power Plants, Vienna (2016).

[15] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Energy Series: No. NP-T-3.12: Core Knowledge on Instrumentation and Control Systems in Nuclear Power Plants, Vienna (2011).

[16] ASSANTE, M. J. et al., "The Case for Simplicity in Energy Infrastructure," Center for Strategic and International Studies (2015) http://csis.org/publication/case-simplicity-energy-infrastructure

[17] DANZIG, R. J., "Surviving on a Diet of Poisoned Fruit," Center for a New American Security (2014) www.cnas.org/sites/default/files/publications-pdf/CNAS_PoisenedFruit_Danzig_0.pdf

[18] RICHARDS, R., "High-Assurance Cyber Military Systems (HACMS)," http://www.darpa.mil/program/high-assurance-cyber-military-systems

[19] UNITED STATES DEPARTMENT OF HOMELAND SECURITY, "A Roadmap for Cybersecurity Research," (2009), https://www.dhs.gov/sites/default/files/publications/CSD-DHS-Cybersecurity-Roadmap.pdf.

[20] VOAS, J., and SCHAFFER, K., "Insights on Formal Methods in Cybersecurity," *Computer,* vol. 49, no. 5, pp. 102-105, 2016.

[21] "Atelier B 4.0," Atelier B. (2016), http://www.atelierb.eu/en

[22] ROXEY, T., personal communication, December 2015.

[23] SWEARINGEN, M., et al., "What You Need to Know (and Don't) About the AURORA Vulnerability," Power (2013), http://www.powermag.com/what-you-need-to-know-and-dont-about-the-aurora-vulnerability/