Cybersecurity for Small Modular Reactors (SMRs): Regulatory Challenges and Opportunities

Cristina Siserman-Gray, Pacific Northwest National Laboratory (PNNL)

Guy Landine, Pacific Northwest National Laboratory (PNNL)

Abstract

Ensuring the security of nuclear facilities has been a critical element in preventing theft of nuclear materials and sabotage that could result in a radiological release. In the past decade, addressing the threat of a cyber-attack on a facility that could lead to either an act of theft or sabotage has been presenting technical and regulatory challenges to operators as well as national authorities. In this context, the forthcoming arrival of small modular reactors (SMRs) and other advanced nuclear reactor technologies has raised a series of questions as to whether the international and national legal frameworks are prepared to address the cybersecurity challenges associated with this new type of technology. The objective of this paper is threefold: 1) identify gaps and challenges in addressing cybersecurity implications for SMRs; 2) conduct a brief analysis on cybersecurity national regulatory perspectives and identify best practices; 3) provide a series of recommendations on how these challenges could be potentially mitigated from a regulatory perspective. The paper will put forward the idea that for addressing the cybersecurity challenges associated with SMRs strong adaptative regulatory mechanisms, as well as international cooperation are vital.

Keywords: cybersecurity, Advanced Reactors, legal and regulatory framework etc.

1. Introduction

Small Modular Reactors (SMRs) are a class of advanced nuclear fission reactors comprised of factory-built components and systems that are transported as modules and installed at a licensee's site. The term SMR reflects the size, capacity, and modularity of the construction of the reactor and is not indicative of the specific nuclear process used within the design. The International Atomic Energy Agency (IAEA) defines SMRs as reactors with electric generating capacity of 300 megawatts (MWe) and below. SMRs are considered to be the nuclear energy of the future. It is believed that this type of reactors could be key in helping countries achieve their net-zero goals, as they are estimated to be less expensive and safer to operate than traditional nuclear reactors which typically produce more than 500 MWe[1]. If successfully deployed, SMRs will provide clean energy integration with the grid, while working synergistically with renewable energy sources such as solar and wind[2].

Today, most existing nuclear power plants (NPP) around the world use a combination of digital and analog systems to monitor, operate, control and protect the facility[3]. Digital assets, systems, and networks associated with safety-related and security functions are typically air-gapped or protected from cyber threats originating

[1] Aamoth, B., Lee, W., Ahmed, H., *Net-Zero Through Small Modular Reactors - Cybersecurity Considerations*, IECON 2022 – 48th Annual Conference of the IEEE Industrial Electronics Society, Brussels, Belgium, 2022, p. 1, https://ieeexplore.ieee.org/document/9968304 (accessed April 2023).

[2] Fasano, R., *Cyber-Physical Risks for Advanced Reactors*, Sandia National Lab. (SNL-NM), Albuquerque, NM (United States), 2021, https://www.osti.gov/servlets/purl/1854721 (accessed April 2023).

[3] Chowdhury, N., *Cybersecurity measures for nuclear power plant protection: A systematic literature review*, Signals, Vol. 2, No. 4, p. 803, https://ntnuopen.ntnu.no/ntnu-xmlui/handle/11250/2829013 (accessed April 2023).

from non-plant or external networks, including the Internet[4], by implementing security controls such as data-diodes and firewalls. However, it is important to recognize that, while an air gap can introduce additional complexity into the attack path planning, it will not stop all malicious attacks, and facilities continue to be exposed to cybersecurity vulnerabilities.[5] Incidents of cyber-attacks on computer systems, across all industries, are a common occurrence and are reported regularly in the media[6]. In the past decades, several reports[7] exposed the growing risk of a cyber-attack on civil nuclear facilities because of the increased reliance on digital systems and the growing use of "off-the-shelf" software and equipment, as well as vulnerabilities in the supply chain[8].

Similar to traditional nuclear power plants, SMRs designs anticipate the use of semi-autonomous or highly automated control systems composed of digital components such as wireless monitoring, digital communications, remote or shared data processing and modern control-system components[9]. With new SMRs designs anticipating a potential for remote use, portability of the systems, and critical digital process control, the existing design-basis threat analysis will have to be adapted to account for disruptive failures of automated technology and malicious threats, such as targeted cyberattacks. In this context, cyber-physical security risk management for SMRs is an active area of research and regulatory concern.

SMR concepts are currently at very different stages of development. While most of them only exist as concept studies, in several countries, SMR designs have already been certified by regulatory authorities on their safety design, and contracts for the construction of such plants have been signed (e.g., USA, Britain, Romania or Poland). Given that many governments are just beginning to grapple with the emerging cybersecurity risk specific to nuclear industry, regulatory standards are insufficient in addressing cybersecurity. In effect, only a small number of countries have issued regulatory requirements or other standards on cybersecurity at nuclear facilities, and even the few existing ones, do not contain specific cybersecurity references to SMR technology[10]. While this is understandable, given that the SMR technology is relatively new, it is however recommended that special attention is dedicated to this area as more regulators will have to go through the process of certifying SMRs as more designs are developed. This paper first identifies and analyses several cybersecurity vulnerabilities applicable to SMRs. Then, it highlights several cybersecurity national regulatory approaches and best practices that international organizations and

[4] D. Livingstone, C. Baylon, R. Brunt, *Cyber Security at Civil Nuclear Facilities: Understanding the Risks*, Chatham House Research Institute of International Affairs, 2015, https://www.chathamhouse.org/publication/cyber-security-civil-nuclear-facilitiesunderstanding-risks (accessed April 2023).
[5] Sabharwall, P., *Cyber security for microreactors in advanced energy systems*, Cybersecurity: A peer-Reviewed Journal, Vol. 4, p. 350, available at: https://gain.inl.gov/SiteAssets/MicroreactorProgram/CyberSecurityForMicroreactorsInAdvancedEnergySystems.pdf (accessed April 2023)
[6] Busquim, R., Kubelwa, N., *SMR Digital Technologies and Computer Security: The Interlinkages*, 2022, available https://www.iaea.org/newscenter/news/smr-digital-technologies-and-computer-security-the-interlinkages (accessed April 2023).
[7] D. Livingstone, C. Baylon, R. Brunt, *Cyber Security at Civil Nuclear Facilities: Understanding the Risks*, Chatham House Research Institute of International Affairs, 2015, available at: https://www.chathamhouse.org/publication/cyber-security-civil-nuclear-facilitiesunderstanding-risks (accessed April 2023).
[8] Duguay, R., *Small Modular Reactors and Advanced Reactor Security: Regulatory Perspectives on Integrating Physical and Cyber Physical and Cyber Security by Design to Protect Against Malicious Acts and Evolving Threats*, International Journal of Nuclear Security, Vol. 7, No. 1, Article 2, p. 42, available at: https://trace.tennessee.edu/cgi/viewcontent.cgi?article=1132&context=ijns (accessed April 2023).
[9] *Ibid.*
[10] Pickering, S., Davies, P., *Cyber Security of Nuclear Power Plants: US and Global Perspectives*, Georgetown Journal of International Affairs, 2021, https://gjia.georgetown.edu/2021/01/22/cyber-security-of-nuclear-power-plants-us-and-global-perspectives/ (accessed April 2023).

several countries have proposed to address these challenges. Lastly, it identifies a series of recommendations on how these cybersecurity challenges could be potentially mitigated from a legal and regulatory perspective.

2. Cybersecurity risks and vulnerabilities for SMRs

SMRs are expected to be very flexible as they can be scaled up or down to meet the energy demands and help power areas where larger plants are not needed. Yet, these nuclear technologies can be very different from the current operating nuclear fleet, as they are relying on digitally controlled operations, miniaturization of components, wireless and automated technologies, as well as artificial intelligence, all providing the promise of delivering innovative solutions for complying with nuclear security standards for SMRs[11]. At the same time, their use also presents several significant cybersecurity challenges, which will be discussed in the following section.

2.1 Remote Supervisory Control

It appears that many companies developing SMRs intend to operate them in a mostly remote manner. This is likely driven by the potential for cost savings. Some potential use-cases for SMRs may include siting these reactors in "off-grid" locations such as isolated communities, remote mining camps, and distant industrial sites that require consistent and reliable power generation. Use of SMRs in such environments would necessitate remote operation and monitoring of the deployed reactors by licensed operators presumably located a considerable distance from the site. This poses a challenge as existing IAEA guidance effectively recommends that “command and control” of the reactor be conducted from a main control room located within the protected area of a site by a sizeable team of licensed operators[12]. Until now, the subject of remote operation of a commercial nuclear reactor was never envisioned or contemplated. As such, it represents a “paradigm shift” with respect to traditional nuclear plant operations[13].

Cyber security regulations associated with traditional NPPs characteristically require licensees to develop, apply, and maintain defense-in-depth protective strategies capable of detecting, responding to, and recovering from cyber-attacks. Central to these strategies is the implementation of a data flow model defining acceptable types of communications flowing between digital systems maintained at different security levels within the facility[14]. To facilitate such data transfer, it is recommended that licensees implement a robust Defensive Computing Security Architecture (DCSA) using devices and mechanisms to ensure that systems performing significant safety and security functions have the requisite level of protection[15]. Communications necessary to support command and control functions from an offsite location (e.g., a remote-control room) appear to be incompatible with SMRs data flow models.

Remote operation of SMRs also creates an adversarial pathway or vector of attack that was otherwise mitigated by onsite control rooms. Because control of the physical communications medium extends far beyond the physical boundaries of the site, it no longer inherits the benefits of the plant’s Physical Protection

[11] Busquim, R., Kubelwa, N., *SMR Digital Technologies and Computer Security: The Interlinkages*, 2022, available https://www.iaea.org/newscenter/news/smr-digital-technologies-and-computer-security-the-interlinkages (accessed April 2023).
[12] IAEA, *Computer Security Techniques for Nuclear Facilities*, NSS-17-T (Rev.1), 2021, https://www-pub.iaea.org/MTCD/Publications/PDF/PUB1921_web.pdf (accessed April 2023).
[13] US NRC, *Ground Rules for Regulatory Feasibility of Remote Operations of Nuclear Power Plants*, https://www.nrc.gov/docs/ML2129/ML21291A024.pdf (accessed April 2023).
[14] US NRC, Regulatory Guide 5.71, Revision 1 *Cyber Security Programs for Nuclear Power Reactors*, USNRC https://www.nrc.gov/docs/ML2225/ML22258A204.pdf (accessed April 2023).
[15] International Atomic Energy Agency, *Computer Security of Instrumentation and Control Systems at Nuclear Facilities*, Nuclear Security Series No. 33-T, Vienna, 2018.

System (PPS). As such, certain disruptive attacks cannot be effectively prevented and may not be responded to in a timely manner. The severity of such an event is dependent upon the systems involved, the functions that they provide, and consequences resulting from loss or impairment of those functions.

Additionally, a new dependency relationship likely exists with an external entity, specifically that of a telecommunications provider to facilitate communications between the reactor and the remote-control room. This could create significant issues from both a liability and a regulatory perspective. For instance, if a service disruption or misconfiguration occurs on the network owned by the telecommunication provider that results in damage or loss of generation capacity of the reactor, legal questions arise on the financial liability being assumed. Further, since the telecommunication provider may have the ability to impact reactor operations by virtue of the newly established telecommunications link, the issue of whether the telecommunications provider should become a regulated entity under the Competent Authority also becomes a relevant question.

2.2 Autonomous Operations

Operating costs associated with NPPs has historically been expensive. According to the World Nuclear Organization (WNO), Operations and Maintenance (O&M) costs account for approximately 66% of the total operating cost of an NPP[16]. A significant percentage of this cost can be attributed to the large number of operations and technical personnel required to operate, calibrate, maintain, and test various plant systems to ensure their functionality. These staffing requirements are primarily driven by resource demands to respond to transients and accidents and are based on traditional operational models with limited automation[17]. To avoid the prospect that high staffing levels relative to unit power production will lead to unsustainable O&M costs for SMRs, a significantly higher degree of automation will be necessary[18].

It is important to note that much of the recent developments regarding autonomous control systems or digital twin technologies[19] are based on using existing off-the-shelf algorithms developed for non-nuclear applications. In this context, the vulnerability of such solutions to infiltrations is relatively higher compared to scenarios in which such technologies are adapted or modified to be more secure, while implemented as an independent solution for each SMR design. Given that SMRs designs are unique to their manufacturers, the vulnerability of a SMR to cyberattack will depend on the specific design of the reactor being attacked.

Regulations concerning licensed operator staffing at nuclear power plants are largely based on the specificities of traditional larger power reactor designs that rely primarily on active safety systems and operator actions to address plant transients and design basis accidents[20]. Highly autonomous reactor designs envisaged for SMRs will interface directly with safety-related and important-to-safety systems and functions. Providing appropriate cybersecurity will be complicated if the design implements an offsite control room to

---

[16] World Nuclear Association, *Economics of Nuclear Power*, https://world-nuclear.org/information-library/economic-aspects/economics-of-nuclear-power.aspx (accessed April 2023).

[17] Wood, R., Upadhyaya, B., Floyd, D., A*n Autonomous Control Framework for Advanced Reactors, Nuclear Engineering and Technology*, 2017.

[18] Wood, R., *Autonomous operation of small reactors: Economy of automation in lieu of economy of scale*, American Nuclear Society, Nuclear Newswire https://www.ans.org/news/article-3037/autonomous-operation-of-small-reactors-economy-of-automation-in-lieu-of-economy-of-scale/ (Accessed April 2023).

[19] Mullheim, M. et al., *Status Report on Regulatory Criteria Applicable to the Use of Digital Twins*, Oak Ridge National Laboratory, 2022, https://info.ornl.gov/sites/publications/Files/Pub179027.pdf (Accessed April 2023).

[20] Belles, R., Mullheim, M., *Licensing Challenges Associated with Autonomous Control*, Oak Ridge National Laboratory, https://info.ornl.gov/sites/publications/Files/Pub120768.pdf (Accessed April 2023).

support a remotely sited reactor[21].Therefore, cybersecurity will be an important consideration for any highly autonomous SMR reactor design to demonstrate adequate physical protection.

2.3 Artificial Intelligence and Machine Learning

Artificial Intelligence (AI) refers to a collection of technologies that produce systems capable of tracking complex problems in ways similar to human logic and reasoning. Machine learning (ML) technologies learn how to complete a particular task based on large amounts of data. Numerous applications for AI/ML exist within NPPs including but not limited to improvements in reactor design, thermal-hydraulic simulation analysis, radiation shielding design, safety, monitoring, operations, and security[22]. Automation via AI/ML is expected to reduce SMR installation costs, shorten construction times and better meet user needs through greater flexibility or non-electric applications.[23]. In this light, the use of AI/ML technologies for SMRs is currently underway[24], with certain vendors already demonstrating prototypes[25].

However, while there are great benefits possible with the use of AI/ML in NPPs, and SMRs alike, there are some potential issues as well that will need to be considered and reflected in regulatory guidance. AI platforms are vulnerable to cyber-attacks and exploitative code is widely available. The attacks targeting ML systems differ significantly when compared to traditional hacks that exploit poorly written code or utilize a vulnerable library. AI systems are vulnerable to a variety of attacks including, including "evasion attacks", in which attackers discover imperfections in the model and then exploit these weaknesses in the deployed model with carefully crafted inputs[26]. Other types of attacks include "data poisoning", in which attackers make changes to the training data to embed malicious patterns for the machine to learn[27], as well as the "model extraction", in which the attacker records the inputs and outputs of the victim model enough times to build a close facsimile of the model to be attacked[28]. In many cases, the vulnerabilities within AI-based systems cannot be patched because the flaw being exploited is related to the fundamental design of the system.

Consequently, it becomes apparent that continuous uses of AI in the nuclear industry, including for SMRs, will rapidly require the transformation of the regulatory landscape. In 2019, there were more than 70 AI regulatory frameworks in existence around the globe, with many other national jurisdictions making significant progress in developing their frameworks in this field.[29] Therefore, these initiatives provide timely opportunities for fresh approaches in the redesign of regulatory systems to keep pace with technological

---

[21] Belles, R., et al., *Licensing Challenges Associated with Autonomous Control*, Oak Ridge National Laboratory, 2018, https://info.ornl.gov/sites/publications/Files/Pub120768.pdf (Accessed April 2023).
[22] Huang, Q. et al., A *review of the application of artificial intelligence to nuclear reactors: Where we are and what's next*, Heliyon, Vol. 9, Issue 3, 2023.
[23] International Atomic Energy Agency, *Artificial intelligence for accelerating nuclear applications, science and technology*, Vienna, 2022. See also IAEA, *New CRP: Technologies Enhancing the Competitiveness and Early Deployment of Small Modular Reactors*, 2022, https://www.iaea.org/newscenter/news/new-crp-technologies-enhancing-the-competitiveness-and-early-deployment-of-small-modular-reactors-i31039 (Accessed April 2023).
[24] Hassan, S. et al, *Machine Learning and Artificial Intelligence-Driven Multi-Scale Modeling for High Burnup Accident-Tolerant Fuels for Light Water-Based SMR Applications*, Electrical Engineering and Systems Science, 2022.
[25] Golchert, B., Banyay, G., *Synopsis of Westinghouse Machine Learning, Artificial Intelligence, and Digital Twin Developments for Nuclear Power Applications*, for the "Workshop on Digital Twin Applications for Advanced Nuclear Technologies", December 2020.
[26] Lohn, A., *Hacking AI A Primer for Policymakers on Machine Learning Cybersecurity, Center for Security and Emerging Technology*, December 2020, https://cset.georgetown.edu/wp-content/uploads/CSET-Hacking-AI.pdf (Accessed April 2023).
[27] Ibid.
[28] Ibid.
[29] Wong, A., *The Laws and Regulation of AI and Autonomous Systems, Unimagined Futures – ICT Opportunities and Challenges*, Springer International Publishing, pp.38-54, 2020, https://inria.hal.science/hal-03194304/document (Accessed April 2023).

changes in the nuclear industry, particularly as it concerns the new generation of SMRs. This includes ensuring regulators' readiness for decision-making in this area, but also establishment of organizational frameworks to review AI applications for these novel technologies.

3. Regulatory Practices and Solutions

There are currently several studies which address the applicability of the international nuclear legal framework to small modular reactors (SMRs)[30]. These studies review the scope and applicability of the international legally binding instruments in the fields of nuclear safety, nuclear liability, nuclear safeguards and non-proliferation, and nuclear security, and discuss the gaps and challenges related to their applicability to SMRs. Consequently, this paper will not rehash the international legal framework associated to SMRs deployment. Instead, it will focus on introducing the relevant IAEA guidance on cybersecurity relevant for SMRs and highlight the regulatory experiences of a select number of countries, which have started to tackle in their regulatory frameworks some the cybersecurity issues identified in the sections above.

3.1 International guidance and standards on cybersecurity

Over the past decade, the IAEA and other international organizations have been actively working to provide guidance and recommendations for cybersecurity of nuclear facilities. Among this guidance, relevant for SMRs, is NSS No. 17 *Computer Security at Nuclear Facilities*, as well as NSS No. 33-T *Computer Security of I&C Systems at Nuclear Facilities*. Using a cyber-risk assessment as a starting point, the IAEA publications recommend cyber requirements based on a risk-informed and graded approach, by addressing the following elements: 1) the importance of Instrumentation and Control (I&C) system functions for both safety and security; 2) the identified and assessed threats to the facility; 3) the attractiveness of the I&C system to potential adversaries; 4) the vulnerabilities of the I&C system; 5) the operating environments. The IAEA is currently spearheading an initiative to support countries on mitigating risks related to the computer security of SMRs[31], many of which will rely on new digital instrumentation and control systems. Also, the SMR Regulators' Forum is expected to provide positions statements on regulatory issues and suggestions for changes to international codes and standards, but for now their worked focused very little on cybersecurity aspects.

Other relevant international standards stem from the International Electrotechnical Commission's (IEC) publication on *Nuclear Power Plant-Implementation and Control Systems for Security Programmes for Computer-based Systems*. This document establishes requirements and provides guidance for the development and management of effective computer security programmes for I&C programmable digital systems. Inherent to these requirements and guidance is the criterion that the power plant I&C programmable digital system security programme complies with the applicable country's requirements.

3.2 National regulatory perspectives on cybersecurity relevant for SMRs

In general, it is observed that across most national jurisdictions, the cybersecurity regulatory framework is more fragmented and complex compared to the nuclear security framework. While some cybersecurity

[30] *See* Kalleveen, V., *Applicability of the international nuclear legal framework to small modular reactors (SMRs)*, JRC Science for Policy Report, 2022, file:///C:/Users/sise584/Downloads/JRC128204_01.pdf; OECD NEA, *Small Modular Reactors: Challenges and Opportunities*, NEA No. 7560, Paris, 2021; Wetherall, A., De Cesar, S., *Developing Internationally and Nationally an Enabling Environment for a Potential Future SMR Deployment,* Nuclear Law Institute, A Collective View on a Decade of Capacity Building and Development in Nuclear Law, 2022.

[31] IAEA, *SMR Digital Technologies and Computer Security: The Interlinkages*, Vienna, 2022, https://www.iaea.org/newscenter/news/smr-digital-technologies-and-computer-security-the-interlinkages (Accessed April 2023).

initiatives in the nuclear industry seem to exist in all countries, these vary considerably, ranging from well-defined and institutionalized approaches, to more fragmented and less formalized one, with some frameworks displaying sporadic and ad hoc approaches[32]. This is possibly due to both historical considerations and the fact that cybersecurity touches extremely varied aspects of a country's infrastructure from telecommunication to intelligence services to national critical infrastructure protection. Even within countries that have put in place a strong cybersecurity framework for traditional nuclear plants, the focus on cyber issues specific to SMRs has only started to surface. In this context, this paper highlights the efforts conducted in the regulatory field by several countries, which have commenced addressing cybersecurity aspects relevant for SMRs.

To begin with, in the United States (USA), shortly after the 9/11 attacks, the Nuclear Regulatory Commission (NRC) issued an order that included cyberattacks among the threats that NPPs would be required to defend against. Additional guidance was released in the next several years, and in 2009 NRC issued cybersecurity regulations under Title 10 of the Code of Federal Regulations (CFR), Section 10 CFR 73.54 *Protection of Digital Computer and Communication Systems and Networks*. A year later, in 2010, Nuclear Energy Institute (NEI) published the implementing guidance NEI 08-09 *Cyber Security Plan for Nuclear Power Reactors*. In accordance with the regulation and guidance, all nuclear power reactor licensees in the US must submit a cyber security plan for approval by the NRC and adhere to regulation which includes inspections[33]. The NRC began inspecting the implementation of plant cybersecurity plans in 2013. Later, the amended version of the Energy Policy Act imposed specific criteria for NRC to consider when revising the Design Basis Threat, to specify the maximum severity of potential attacks that a plant's security force must be capable of repelling.

In July 2020, additional standard requirements pertaining to supply chain risk mitigation were approved by NRC through *Order No. 850*. These mitigation measures require operators to develop, implement and review supply chain plans that account for vendors' remote access, verify software integrity and authenticate code to ensure the code is not counterfeit or modified without knowledge of the software supplier[34]. The requirements establish a comprehensive cyber security program for the protection of digital computer and communications systems and equipment against cyberattacks that would adversely affect operational safety, security, or emergency preparedness. The program includes key cyber security program elements, including the identification of in-scope assets; implementation of security controls; defense-in-depth measures for detection, response, and recovery; managing cyber risks; training; integration of cyber security and physical security programs; development and maintenance of written policies and implementing procedures; reviewing the cyber security program; and records retention[35]. All these requirements would also be applicable to SMRs.

Beyond the US, the topic of cybersecurity in SMRs has been addressed also in other regulatory frameworks. For example, in Canada, the regulatory document REGDOC-2.5.2 *Design of Reactor Facilities: Nuclear Power Plants*, the Canadian Nuclear Safety Commission (CNSC) highlights the importance of interfaces of

[32] Institute for Security and Safety, *Cyber Security at Nuclear Facilities: National Approaches*, University of Applied Sciences, 2015, https://media.nti.org/pdfs/Cyber_Security_in_Nuclear_FINAL_UZNMggd.pdf (accessed April 2023).
[33] Pickering, S., Davies, P., *Cyber Security of Nuclear Power Plants: US and Global Perspectives*, Georgetown Journal of International Affairs, 2021.
[34] Sabharwall, P., *Cyber security for microreactors in advanced energy systems*, Cybersecurity: A peer-Reviewed Journal, Vol. 4, p. 350.
[35] CISA, *Nuclear Sector: Cybersecurity Framework Implementation Guidance*, US Department of Homeland Security, 2020, p. 13. https://www.cisa.gov/sites/default/files/publications/Nuclear_Sector_Cybersecurity_Framework_Implementation_Guidance_FINAL_508.pdf (accessed April 2023).

safety, security, and safeguards for NPP designs. It also ensures that physical protection systems and cyber security programs are considered in NPP design management and documentation[36]. The Canadian Standard Association (CSA) standard *N290.7 Cyber security for nuclear facilities* also applies to SMRs. This standard was developed with the involvement of licensees, the CNSC and other stakeholders[37]. N290.7 contains requirements and guidance for a risk-informed cyber security program to protect against cyber-attack the systems performing functions important to nuclear safety, nuclear security, emergency preparedness and safeguards.

However, a gap analysis conducted by CNSC shows that there remains a need to provide additional guidance and requirements to supplement this standard to ensure that reliable and effective cyber security measures are implemented[38]. In this regard, the CNSC issued a discussion paper titled *Proposals to Amend the Nuclear Security Regulations*[39], which discusses the changes to Nuclear Security Regulations at a high level. Under its effort to modernize the Nuclear Security Regulations and to address evolving threats, CNSC indicated their intention to move toward a performance-based approach with less prescriptive requirements. In the country's view, this more flexible approach will allow adaptation to an evolving security environment, such as the rapidly evolving threats of cyber-attacks[40].

Among the European countries, the United Kingdom is one of the leading countries in the international effort to address in its regulatory framework cybersecurity aspects to SMRs, but is still in the process to update its regulatory framework to include this aspect. The 2021 National Cyber Strategy sets the United Kingdom (UK) as the aspiring global leader in cyber power, while also protecting UK's interests in cyberspace. That vision is matched in the civil nuclear sector, with this strategy sitting underneath the national framework and supporting its delivery[41]. The *2020 Energy White Paper*[42], the *Prime Minister's 10 Point Plan for a Green Revolution*[43], *the 2021 Net Zero Strategy*[44] and the *2022 British Energy Security Strategy*[45] all stated the government's objective to advance nuclear as a secure and clean energy source through development of both large-scale nuclear and the next generation of SMRs[46].

---

[36] Lei, Y., *Assessing Cyber Security in Small Modular Reactors*, Canadian Nuclear Safety Commission, November 2019, https://nuclearsafety.gc.ca/eng/resources/research/technical-papers-and-articles/2019/assessing-cyber-security-smrs.cfm.

[37] CNSC, *Cyber Security and the Protection of Digital Information*, Discussion Paper DIS-21-03, 2021, p. 3, https://www.nuclearsafety.gc.ca/eng/pdfs/Discussion-Papers/21-03/Discussion_Paper_DIS-21-03__Cyber_Security_and_the_Protection_of_Digital_Information.pdf (accessed April 2023).

[38] Ibid, p. 44.

[39] CNSC, *Cyber Security and the Protection of Digital Information*, Discussion Paper DIS-21-03, 2021.

[40] Duguy, R., Ibid, p. 22.

[41] UK Department of Business, Energy and Industrial Strategy, *2022 Civil Nuclear Cyber Security Strategy*, 2022, p. 5, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1075002/civil-nuclear-cyber-security-strategy-2022.pdf

[42] Department for Energy Security and Net Zero and Department for Business, Energy & Industrial Strategy, *Energy white paper: Powering our net zero future*, December 2020, https://www.gov.uk/government/publications/energy-white-paper-powering-our-net-zero-future.

[43] Department for Energy Security and Net Zero and Department for Business, Energy & Industrial Strategy, *The ten point plan for a green industrial revolution*, November 2020, https://www.gov.uk/government/publications/the-ten-point-plan-for-a-green-industrial-revolution.

[44] Department for Energy Security and Net Zero and Department for Business, Energy & Industrial Strategy, *Net Zero Strategy: Build Back Greener*, 2021, https://www.gov.uk/government/publications/net-zero-strategy.

[45] Department for Energy Security and Net Zero and Department for Business, Energy & Industrial Strategy, *British energy security strategy*, April 2022, https://www.gov.uk/government/publications/british-energy-security-strategy#:%7E:text=The%20'British%20energy%20security%20strategy,as%20Russia's%20invasion%20of%20Ukraine.

[46] Helsketh, K., Barron, N., *Small modular reactors (SMRs): The case of the United Kingdom*, Handbook of Small Modular Reactors, Woodhead Publishing in Energy, 2021, p. 503-520.

As part of a techno-economical assessment of SMR designs, the Office of Nuclear Regulation (ONR) performed a pre–Generic Design Assessment (GDA) with the objective to identify issues and challenges that could arise if an SMR was submitted to a GDA process, and to develop possible arguments by which these challenges might be addressed. In view of performing the GDA assessment, ONR reviewed UK regulatory principles, guides, and published reports on the outcome of GDAs for large reactors with the objective to identify issues likely to be raised by regulators in a GDA of an SMR. The list of potentially significant issues, including cybersecurity aspects, was validated at workshops and meetings held with ONR[47]. The UK committed to engage closely with SMR developers on cybersecurity considerations as advanced nuclear technologies continue to develop to ensure that the ONR's GDA process has cyber and information security requirements built in[48]. While currently there are no cybersecurity provisions included in UK regulations that specifically reference SMRs, assessment initiatives as GDA represent a best practice for other States considering deploying or acquiring SMRs.

4. Recommendations and potential path forward

As highlighted in the previous sections, cybersecurity regulations released by government authorities, including those highlighted here, tend to discuss SMRs-related cybersecurity at a high level, if at all, and typically do not go into detail about specific threats and vulnerabilities. Therefore, a cyber regulatory framework addressing SMRs must be factored in for this type of technology to be robust, diverse and proactive to future challenges. In the following section, we propose several options for regulators to address cybersecurity aspects for SMRs.

4.1. Cybersecurity requirements in Prescriptive vs. Performance-Based Regulations

It is important for regulators to become aware that the threat that the nuclear sector faces in cyberspace, particularly for SMRs, is rapidly changing, requiring thus a powerful and agile response mechanism reflected in the regulatory frameworks. In this context, the selection of the regulatory approach influences the organizational structure and size of the regulatory body and consequentially will have a major influence on the resources needed. Some countries, including USA, endorse a regulatory framework based on performance requirements that minimize or eliminate prescriptive requirements with the objective of permitting the applicant or licensee the maximum flexibility to determine how it will design and implement the necessary cybersecurity protection. Performance-based security assessments may be developed using risk-informed plant design features which will demonstrate that cybersecurity design requirements are fully integrated throughout the entire design and licensing process. Regulators and the nuclear industry are encouraged to consider, within their existing regulatory frameworks, performance outcome-based approaches for all SMRs, which recognizes and incentivizes reducing the exposure to security risks due to the SMRs' integrated safety and security features[49].

4.2 Harmonization of cyber national regulatory practices

Given the cybersecurity vulnerabilities discussed above, another solution would be the harmonization of national approaches and regulations on cybersecurity aspects to make the international market for SMRs more viable, and, thus, reconfirm the need for maintenance of cybersecurity measures during the SMR's

[47] UK Department of Business, Energy and Industrial Strategy TEA Project 4 Vol 1 – Assessment of UK regulatory regime for SMRs, 2016, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/665298/TEA_Project_4_Vol_1_-_Assessment_of_UK_Regulatory_Regime_for_SMRs.pdf

[48] UK Department of Business, Energy and Industrial Strategy, *2022 Civil Nuclear Cyber Security Strategy*, 2022, p. 24.

[49] Nuclear Energy Institute, *Position Paper: Physical Security for Small Modular Reactors*, 2012, p. 8.

lifecycle, starting from design to decommissioning[50]. Harmonization of standards is a process intended to minimize conflicting and repetitive requirements between standards in multiple jurisdictions[51]. At a general level, harmonized standards are intended to capture common or fundamental requirements among national, regional, and international bodies. From a regulatory perspective, the main objective of SMR cybersecurity harmonization would be to increase regulatory collaboration, and to establish common positions on technical and policy issues in the pre-licensing phase for SMRs[52]. An international cybersecurity standard to be applicable to SMRs would have the merit of documenting a globally accepted set of requirements. Some have argued that regulatory frameworks applicable to cybersecurity would face several challenges, the most immediate one regarding each State's DBT and threat assessments, which are confidential and subject to each State's evolving threat environments. In this regard, it would be useful to promote efforts to authorize the regulators to exchange information and cooperate with regulatory bodies in other States and with relevant international organizations concerning cybersecurity aspects relevant for SMRs. Given that this is an area that has not yet receive much attention in the specialized literature, it would be deserving of more attention in the near future.

4.3 Inclusion of cybersecurity-by-design regulatory requirements

The application of cybersecurity-by-design[53] principles for SMRs designs could provide regulators with the opportunity to request the establishment of a robust and resilient cyber architecture at the beginning of a SMR's life cycle. Currently, there is no incentive for manufacturers and construction companies to invest in cybersecurity by design, as applying the principle of "defense in depth" for cybersecurity at the design stage of an SMR may require the commissioning of technical expertise and investment in design. Including "cybersecurity-by-design" principles into regulatory requirement would ensure that this aspect is covered in the early design phases.

An important aspect of cybersecurity-by-design has to do with managing the cyber supply chain. With cyber components being manufactured and assembled in locations across the world, it is expected that the licensee will be less able to supervise the process and ensure quality. The increased number of individuals and organizations with access to the components used in the SMR presents cyber-risks, as there are more opportunities for cyber vulnerabilities to be introduced into the supply chain and components[54]. This will be especially concerning for small countries and less-developed countries that must rely almost exclusively on suppliers from other countries that may apply different supply chain standards on cyber components.

The International Atomic Energy Agency (IAEA) has produced guidance to help manage risks from counterfeit and fraudulent items in the nuclear industry but notes the continuing challenges, from original providers ending system updates to actors deliberately diverting and substituting fraudulent integrated

[50] Busquim, R., Kubelwa, N., *SMR Digital Technologies and Computer Security: The Interlinkages*, 2022.
[51] Marotta, A., Madnick, S., *Convergence and divergence of regulatory compliance and Cybersecurity*, Issues in Information Systems, Vol. 22, Issue 1, 0.10-50, 2021, https://www.iacis.org/iis/2021/1_iis_2021_10-50.pdf.
[52] Donovan, J., Vives, P., *Accelerating SMR Deployment: New IAEA Initiative on Regulatory and Industrial Harmonization*, April 2022, https://www.iaea.org/newscenter/news/accelerating-smr-deployment-new-iaea-initiative-on-regulatory-and-industrial-harmonization.
[53] Brunt, R., Unal, B., *Cybersecurity by Design in Civil Nuclear Power Plants*, Chatham House, 2019, https://www.chathamhouse.org/sites/default/files/2019-07-23-Cybersecurity-Nuclear-Power-Plants.pdf.
[54] U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency, *Nuclear Sector: Cybersecurity Implementation Guidance*, May 2020, p. 15, https://www.cisa.gov/sites/default/files/publications/Nuclear_Sector_Cybersecurity_Framework_Implementation_Guidance_FINAL_508.pdf.

circuits for espionage purposes[55]. In light of this, reinforcing the cybersecurity regulations with specific requirements for nuclear industry to address supply-chain vulnerabilities is of high importance[56]. The construction of SMR cybersecurity components will need to go through this rigorous process, which would have to be reflected in the national regulatory frameworks. This entails using reliable manufacturers and implementing effective provisions to protect confidentiality, integrity, and availability of the information and assets, as well as to prevent backdoor intrusions and denial of service.

5. Conclusions

While SMR's appear to have great potential in terms of economically generating power and reducing CO2 emissions, the cybersecurity risks associated with SMRs appear to be greater than those associated with more traditional nuclear reactors. However, given the growing interest from multiple countries to deploy SMRs in the near future, there is a compelling need for regulatory requirements and standards, as well as operational guidance to tackle the cybersecurity vulnerabilities associated with these new technologies. Considering how difficult it is to fully secure any digital system, remote SMR operation would undoubtedly present new cybersecurity vulnerabilities that the nuclear energy community will have to mitigate through robust regulatory framework. Therefore, it is advisable that as regulators continue to regulate in this field, they engage the SMR industry to develop and implement strong cyber programs that address cybersecurity vulnerabilities from the inception to the decommissioning of these technologies.

References

Aamoth, B., Lee, W., Ahmed, H., *Net-Zero Through Small Modular Reactors - Cybersecurity Considerations*, IECON 2022 – 48th Annual Conference of the IEEE Industrial Electronics Society, Brussels, Belgium, 2022, p. 1, https://ieeexplore.ieee.org/document/9968304 (accessed April 2023).

Belles, R., Mullheim, M., *Licensing Challenges Associated with Autonomous Control*, Oak Ridge National Laboratory, https://info.ornl.gov/sites/publications/Files/Pub120768.pdf (Accessed April 2023).

Brunt, R., Unal, B., *Cybersecurity by Design in Civil Nuclear Power Plants*, Chatham House, 2019, https://www.chathamhouse.org/sites/default/files/2019-07-23-Cybersecurity-Nuclear-Power-Plants.pdf. (accessed April 2023).

Busquim, R., Kubelwa, N., *SMR Digital Technologies and Computer Security: The Interlinkages*, 2022, available https://www.iaea.org/newscenter/news/smr-digital-technologies-and-computer-security-the-interlinkages (accessed April 2023).

Chowdhury, N., Cybersecurity measures for nuclear power plant protection: A systematic literature review, Signals, Vol. 2, No. 4, p. 803, https://ntnuopen.ntnu.no/ntnu-xmlui/handle/11250/2829013 (accessed April 2023).

CISA, *Nuclear Sector: Cybersecurity Framework Implementation Guidance, US Department of Homeland Security*, 2020, p. 13, https://www.cisa.gov/sites/default/files/publications/Nuclear_Sector_Cybersecurity_Framework_Implementation_Guidance_FINAL_508.pdf (accessed April 2023).

[55] IAEA, Managing Counterfeit and Fraudulent Items in the Nuclear Industry, Nuclear Energy Series no NP-T-3.26, IAEA, Vienna, 2019.
[56] Pham, T., *Updated NIST Cybersecurity Framework Emphasizes Access Control & Supply Chain Risk*, Decipher, May 3, 2018, https://duo.com/decipher/updated-nist-cybersecurity-framework-emphasizes-access-control-and-supply-chain-risk.

CNSC, *Cyber Security and the Protection of Digital Information*, Discussion Paper DIS-21-03, 2021, p. 3, https://www.nuclearsafety.gc.ca/eng/pdfs/Discussion-Papers/21-03/Discussion_Paper_DIS-21-03__Cyber_Security_and_the_Protection_of_Digital_Information.pdf (accessed April 2023).

D. Livingstone, C. Baylon, R. Brunt, *Cyber Security at Civil Nuclear Facilities: Understanding the Risks*, Chatham House Research Institute of International Affairs, 2015, https://www.chathamhouse.org/publication/cyber-security-civil-nuclear-facilitiesunderstanding-risks (accessed April 2023).

Department for Energy Security and Net Zero and Department for Business, Energy & Industrial Strategy, *Energy white paper: Powering our net zero future*, December 2020, https://www.gov.uk/government/publications/energy-white-paper-powering-our-net-zero-future (accessed April 2023).

Department for Energy Security and Net Zero and Department for Business, Energy & Industrial Strategy, *The ten point plan for a green industrial revolution*, November 2020, https://www.gov.uk/government/publications/the-ten-point-plan-for-a-green-industrial-revolution (accessed April 2023).

Department for Energy Security and Net Zero and Department for Business, Energy & Industrial Strategy, *Net Zero Strategy: Build Back Greener*, 2021, https://www.gov.uk/government/publications/net-zero-strategy (accessed April 2023).

Department for Energy Security and Net Zero and Department for Business, Energy & Industrial Strategy, *British energy security strategy*, April 2022, https://www.gov.uk/government/publications/british-energy-security-strategy#:%7E:text=The%20'British%20energy%20security%20strategy,as%20Russia's%20invasion%20of%20Ukraine (accessed April 2023).

Donovan, J., Vives, P., *Accelerating SMR Deployment: New IAEA Initiative on Regulatory and Industrial Harmonization*, April 2022, https://www.iaea.org/newscenter/news/accelerating-smr-deployment-new-iaea-initiative-on-regulatory-and-industrial-harmonization (accessed April 2023).

Duguay, R., *Small Modular Reactors and Advanced Reactor Security: Regulatory Perspectives on Integrating Physical and Cyber Physical and Cyber Security by Design to Protect Against Malicious Acts and Evolving Threats*, International Journal of Nuclear Security, Vol. 7, No. 1, Article 2, p. 42, available at: https://trace.tennessee.edu/cgi/viewcontent.cgi?article=1132&context=ijns (accessed April 2023).

Fasano, R., *Cyber-Physical Risks for Advanced Reactors*, Sandia National Lab, Albuquerque, NM (United States), 2021, https://www.osti.gov/servlets/purl/1854721 (accessed April 2023).

Golchert, B., Banyay, G., *Synopsis of Westinghouse Machine Learning, Artificial Intelligence, and Digital Twin Developments for Nuclear Power Applications, for the "Workshop on Digital Twin Applications for Advanced Nuclear Technologies*, December 2020.

Hassan, S. et al, *Machine Learning and Artificial Intelligence-Driven Multi-Scale Modeling for High Burnup Accident-Tolerant Fuels for Light Water-Based SMR Applications*, Electrical Engineering and Systems Science, 2022.

Helsketh, K., Barron, N., *Small modular reactors (SMRs): The case of the United Kingdom*, Handbook of Small Modular Reactors, Woodhead Publishing in Energy, 2021, p. 503-520.

Huang, Q. et al., *A review of the application of artificial intelligence to nuclear reactors: Where we are and what's next*, Heliyon, Vol. 9, Issue 3, 2023.

International Atomic Energy Agency, *Computer Security Techniques for Nuclear Facilities, NSS-17-T (Rev.1)*, 2021, https://www-pub.iaea.org/MTCD/Publications/PDF/PUB1921_web.pdf (accessed April 2023).

International Atomic Energy Agency, *Managing Counterfeit and Fraudulent Items in the Nuclear Industry*, Nuclear Energy Series no NP-T-3.26, IAEA, Vienna, 2019.

Institute for Security and Safety, *Cyber Security at Nuclear Facilities: National Approaches, University of Applied Sciences*, 2015, https://media.nti.org/pdfs/Cyber_Security_in_Nuclear_FINAL_UZNMggd.pdf (accessed April 2023).

International Atomic Energy Agency, *Artificial intelligence for accelerating nuclear applications, science and technology*, Vienna, 2022.

International Atomic Energy Agency, *Computer Security of Instrumentation and Control Systems at Nuclear Facilities*, IAEA Nuclear Security Series No. 33-T, IAEA, Vienna, 2018.

International Atomic Energy Agency, *New CRP: Technologies Enhancing the Competitiveness and Early Deployment of Small Modular Reactors*, 2022, https://www.iaea.org/newscenter/news/new-crp-technologies-enhancing-the-competitiveness-and-early-deployment-of-small-modular-reactors-i31039 (Accessed April 2023).

Kalleveen, V., *Applicability of the international nuclear legal framework to small modular reactors (SMRs), JRC Science for Policy Report*, 2022, file:///C:/Users/sise584/Downloads/JRC128204_01.pdf (Accessed April 2023).

Lei, Y., *Assessing Cyber Security in Small Modular Reactors*, Canadian Nuclear Safety Commission, November 2019, https://nuclearsafety.gc.ca/eng/resources/research/technical-papers-and-articles/2019/assessing-cyber-security-smrs.cfm (accessed April 2023).

Lohn, A., *Hacking AI A Primer for Policymakers on Machine Learning Cybersecurity*, Center for Security and Emerging Technology, December 2020, https://cset.georgetown.edu/wp-content/uploads/CSET-Hacking-AI.pdf (Accessed April 2023).

Marotta, A., Madnick, S., *Convergence and divergence of regulatory compliance and Cybersecurity*, Issues in Information Systems, Vol. 22, Issue 1, 0.10-50, 2021, https://www.iacis.org/iis/2021/1_iis_2021_10-50.pdf (accessed April 2023).

Mullheim, M. et al., *Status Report on Regulatory Criteria Applicable to the Use of Digital Twins*, Oak Ridge National Laboratory, 2022, https://info.ornl.gov/sites/publications/Files/Pub179027.pdf (Accessed April 2023).

Nuclear Energy Institute, Position Paper: Physical Security for Small Modular Reactors, 2012, p. 8.

OECD NEA, *Small Modular Reactors: Challenges and Opportunities*, NEA No. 7560, Paris, 2021, https://www.oecd-nea.org/upload/duntocs/application/pdf/2021-03/7560_smr_report.pdf (Accessed April 2023).

Pham, T., *Updated NIST Cybersecurity Framework Emphasizes Access Control & Supply Chain Risk*, Decipher, May 3, 2018, https://duo.com/decipher/updated-nist-cybersecurity-framework-emphasizes-access-control-and-supply-chain-risk (accessed April 2023).

Pickering, S., Davies, P., *Cyber Security of Nuclear Power Plants: US and Global Perspectives*, Georgetown Journal of International Affairs, 2021, https://gjia.georgetown.edu/2021/01/22/cyber-security-of-nuclear-power-plants-us-and-global-perspectives/ (accessed April 2023).

Sabharwall, P., *Cyber security for microreactors in advanced energy systems*, Cybersecurity: A peer-Reviewed Journal, Vol. 4, p. 350, available at: https://gain.inl.gov/SiteAssets/MicroreactorProgram/CyberSecurityForMicroreactorsInAdvancedEnergySystems.pdf (accessed April 2023)

U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency, *Nuclear Sector: Cybersecurity Implementation Guidance*, May 2020, p. 15, https://www.cisa.gov/sites/default/files/publications/Nuclear_Sector_Cybersecurity_Framework_Implementation_Guidance_FINAL_508.pdf (accessed April 2023).

UK Department of Business, *Energy and Industrial Strategy TEA Project 4 Vol 1 – Assessment of UK regulatory regime for SMRs*, 2016, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/665298/TEA_Project_4_Vol_1_-_Assessment_of_UK_Regulatory_Regime_for_SMRs.pdf (accessed April 2023).

UK Department of Business, Energy and Industrial Strategy, *2022 Civil Nuclear Cyber Security Strategy*, 2022, p. 5, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1075002/civil-nuclear-cyber-security-strategy-2022.pdf (accessed April 2023).

UK Department of Business, Energy and Industrial Strategy, *2022 Civil Nuclear Cyber Security Strategy*, 2022, p. 24.

US NRC, *Ground Rules for Regulatory Feasibility of Remote Operations of Nuclear Power Plants*, https://www.nrc.gov/docs/ML2129/ML21291A024.pdf (accessed April 2023).

US NRC, *Regulatory Guide 5.71, Revision 1 Cyber Security Programs for Nuclear Power Reactors*, https://www.nrc.gov/docs/ML2225/ML22258A204.pdf (accessed April 2023).

Wetherall, A., De Cesar, S., *Developing Internationally and Nationally an Enabling Environment for a Potential Future SMR Deployment*, Nuclear Law Institute, A Collective View on a Decade of Capacity Building and Development in Nuclear Law, 2022, https://inis.iaea.org/search/search.aspx?orig_q=RN:53049186 (Accessed April 2023).

Wong, A., *The Laws and Regulation of AI and Autonomous Systems, Unimagined Futures – ICT Opportunities and Challenges*, Springer International Publishing, pp.38-54, 2020, https://inria.hal.science/hal-03194304/document (Accessed April 2023).

Wood, R., *Autonomous operation of small reactors: Economy of automation in lieu of economy of scale*, American Nuclear Society, Nuclear Newswire, https://www.ans.org/news/article-3037/autonomous-operation-of-small-reactors-economy-of-automation-in-lieu-of-economy-of-scale/ (Accessed April 2023).

Wood, R., Upadhyaya, B., Floyd, D., *An Autonomous Control Framework for Advanced Reactors*, Nuclear Engineering and Technology, 2017.

World Nuclear Association, *Economics of Nuclear Power*, https://world-nuclear.org/information-library/economic-aspects/economics-of-nuclear-power.aspx (accessed April 2023).