NRC Regulatory Efforts for Cybersecurity

of Small Modular Reactors

Tammie Rivera

U.S. Nuclear Regulatory Commission (NRC)

Rockville, Maryland, United States of America

Email: Tammie.Rivera@nrc.gov

Ismael Garcia

U.S. NRC

Rockville, Maryland, United States of America

Email: Ismael.Garcia@nrc.gov

**Abstract**

The U.S. Nuclear Regulatory Commission (NRC), supported by cybersecurity experts from the national laboratories, has proposed a technology-inclusive, performance-based, and risk-informed cybersecurity regulatory framework for advanced reactors, including small modular reactors (SMRs). This regulatory framework aims to provide a process that accounts for the differing risk levels within SMR technologies, while providing reasonable assurance of adequate protection of public health and safety, promoting the common defense and security, and protecting the environment. A key outcome of the regulatory framework is the establishment of a graded approach that would allow for the development and implementation of a cybersecurity program that protects against unacceptable consequences from a cyberattack.

The paper will discuss and analyze some key assumptions and trends relevant to cybersecurity of SMRs. The NRC expects SMRs to have increased reliance on digital systems, emerging technologies, passive safety features, and other novel design features, such as remote and autonomous operations, which demand reassessment of the applicability of existing paradigms such as network isolation, common in the existing power reactor fleet.

## INTRODUCTION

Current proposed SMR designs involve diverse technologies and have a unique set of functions and systems that support both nuclear safety and security. These technologies, functions, and systems are often different than those used in traditional light water reactors. To address the challenges that come with regulating novel designs, the NRC is moving toward a risk-informed, performance-based, and technology-inclusive regulation and, in parallel, is developing draft guidance (DG) to be used by operators to comply with the new regulation. Section 2 below discusses the efforts associated with the development of the cybersecurity requirements for advanced reactors (ARs), including SMRs, while Section 3 discusses the efforts associated with novel design features and use cases. Finally, Section 4 discusses the efforts and considerations for the future work associated with the proposed cybersecurity requirements and its companion DG.

## Security Concepts

### Background

The NRC licenses and regulates the U.S. civilian use of radioactive materials to provide reasonable assurance of adequate protection of public health and safety, to promote the common defense and security, and to protect the environment. In support of this mission, the NRC establishes regulatory requirements and oversees its licensees’ security programs to ensure special nuclear material, high-level radioactive waste, nuclear facilities, and other radioactive materials are protected from threats, thefts, and sabotage. Title 10 of the Code of Federal Regulations (10 CFR) Part 73, “Physical Protection of Plants and Materials” [1], prescribes requirements for the establishment and maintenance of a physical protection system that will protect special nuclear material at fixed sites and in transit, and for plants that use special nuclear material. Commercial nuclear power plants must implement the physical security requirements in 10 CFR 73.55, “Requirements for Physical Protection of Licensed Activities in Nuclear Power Reactors Against Radiological Sabotage” [2].

As part of the development and implementation of a physical protection program per the requirements in 10 CFR 73.55, commercial nuclear power plant operators need to establish, implement, and maintain a cybersecurity program in accordance with 10 CFR 73.54, “Protection of Digital Computer and Communication Systems and Networks” [3].

The regulations in 10 CFR 73.54 require commercial nuclear power plants operators to ensure that digital computer and communication systems associated with a nuclear power plant’s safety, security, and emergency preparedness (SSEP) functions are protected from cyberattacks. The cybersecurity requirements in 10 CFR 73.54 are based on the functions digital assets perform. Specifically, operators must protect digital assets associated with: (1) SSEP functions and (2) support systems which, if compromised, could adversely impact SSEP functions. Operators must ensure these systems are protected from cyberattacks, up to and including the NRC’s design basis threat, to prevent: (1) adverse impact on integrity/confidentiality of data and software; (2) denial of access to systems, services, and data; and (3) adverse impact to the operations of systems, network, and associated equipment. Regulatory Guide 5.71, “Cyber Security Programs for Nuclear Facilities,” which the NRC originally published in 2010 and updated in 2023 [4], provides guidance on implementing the requirements of 10 CFR 73.54. The Nuclear Energy Institute (NEI) also published implementation guidance in NEI 08-09, “Cyber Security Plan for Nuclear Power Plants” [5]. These documents provide information to aid operators in developing and implementing their cybersecurity plans in accordance with the requirements in 10 CFR 73.54.

### Proposed new cybersecurity requirements

In 2019, President Trump signed the Nuclear Energy Innovation and Modernization Act (NEIMA) into law. NEIMA directed the NRC staff to “complete a rulemaking to establish a technology-inclusive, regulatory framework for optional use by commercial advanced nuclear reactor applicants for new reactor license applications” [6]. In response to NEIMA, the NRC staff is developing a transformative regulatory framework via the development of a new regulation (proposed 10 CFR Part 53[[1]](#footnote-2)), which would build on a strong foundation of Commission policies and decisions and evolves existing requirements into a modern, risk-informed, performance-based approach. Specifically, 10 CFR Part 53 would provide technology-inclusive, risk-informed, performance-based approaches to safety that include scaling the requirements for licensing and regulating a variety of AR designs and technologies. The overall principles associated with this effort include: (1) leveraging the best of the past and developing new tools for the future; (2) crediting technological advancements which could provide operational flexibilities with increased margins of safety; and (3) prioritizing risk-informed and performance-based approaches that accommodate various AR technologies, such as SMRs.

The proposed rule will provide SMR operators the option of either implementing the cybersecurity requirements in 10 CFR 73.54 or those from a new section in 10 CFR Part 73 titled “Technology-Inclusive Requirements for Protection of Digital Computer and Communication Systems and Networks” [7]. The proposed new cybersecurity rule, 10 CFR 73.110, will implement a graded approach based on consequences to determine the level of cybersecurity protection required for AR digital computer and communication systems and network technologies. A graded approach based on potential consequences is intended to facilitate risk-informed approaches, results, and insights for the wide range of reactor technologies to be assessed by the NRC. The rule will recognize the more significant role that may be played by those digital computer and communication systems within future reactor designs. This proposed rule leverages the operating experience and lessons learned from implementation of the current cybersecurity regulations over the past 15 years. The NRC staff submitted its proposed rule to the Commission for approval in March 2023; at time of the publication of this paper, the NRC staff are working to address feedback from the NRC’s Commission, with a goal of finalizing the rule along with the implementation guidance by 2027.

As shown in Fig. 1 below, the proposed new cybersecurity rule at 10 CFR 73.110 will require operators to protect systems associated with functions involving SSEP, using a graded cybersecurity program commensurate with potential consequences from cyberattacks. The first consequence involves radiological sabotage or scenarios involving a cyberattack that adversely impacts the functions of digital assets in a manner that would lead to offsite radiation hazards exceeding established dose criteria, thus endangering public health and safety. The second consequence involves physical intrusion or scenarios involving a cyberattack that adversely impacts the functions performed by physical security digital assets.



FIG. 1. Proposed new cybersecurity approach in 10 CFR 73.110 [8].

Operators would be required to: (1) analyze the potential consequences resulting from cyberattacks and identify those assets that must be protected; and (2) establish, implement, and maintain a cybersecurity program, as defined in the cybersecurity plan, to protect the assets identified by applying defense-in-depth protective strategies to ensure the ability to detect, delay, respond, and recover from cyberattacks capable of causing the stated consequences. In addition, operators would be required to: (1) implement security controls commensurate with safety/security significance via a graded approach; (2) mitigate adverse impacts of cyberattacks capable of causing the stated consequences; and (3) ensure functions of protected assets are not adversely impacted due to cyberattacks capable of causing the stated consequences.

### Draft regulatory guidance development

The NRC, supported by cybersecurity experts from the U.S. Department of Energy national laboratories and U.S. universities, has undertaken efforts to develop a DG [8] to provide a commercial nuclear reactor licensed under 10 CFR Part 53 with an acceptable approach for meeting the requirements of 10 CFR 73.110. Because of the wide range of commercial nuclear plant technologies that may be licensed under 10 CFR Part 53, this DG will establish a new cybersecurity analysis approach than that used by currently operating nuclear power plants in the U.S. This approach includes the following considerations:

1. Commercial nuclear plant designs include increased reliance on digital systems, emerging technologies, passive safety features, and other novel design features.
2. Novel use cases such as remote monitoring and autonomous operations are planned, which demand reassessing legacy systems’ isolation paradigms.
3. This effort is being informed by national and international standards and approaches supporting security concepts having a high degree of expert acceptance, including security design features, customized control catalogs, and performance-based objectives.
4. The increasing capabilities of attackers, with a corresponding increase in sophistication and operational technology focus, dictate a broader approach to software supply chain attacks that includes both technical and administrative defensive measures.

This DG will provide an acceptable method that applies a risk-informed, performance-based, technology-inclusive approach to account for the differing risk levels among commercial nuclear plant technologies to protect against unacceptable consequences from a cyberattack. This DG will describe the elements required in a cybersecurity plan, including a cybersecurity plan template, and contain cybersecurity controls that leverage existing guidance in RG 5.71, which was developed for current light-water commercial nuclear power plants. This effort will also leverage information from the International Atomic Energy Agency and International Electrotechnical Commission publications[[2]](#footnote-3). The following sections provide a high-level overview of the approach being developed as part of this DG.

This DG will implement a three-tier approach via analyses at the facility level, function level, and system level. At the facility level, the intent of the analysis is to rely on existing safety and security assessments to determine if the plant’s design basis and existing physical protection systems are sufficient to effectively prevent potential consequences from a cyberattack. At the function level, the intent of the analysis is to understand the adversary’s potential access to attack pathways that allow for the compromise of plant functions resulting in unacceptable consequences, as defined in 10 CFR 73.110. At the system level, the intent of the analysis is to identify protective measures, including system-level cybersecurity controls, to prevent or mitigate the impact to compromised plant functions.

Both the functional level and system level analyses will employ the use of a graded approach to determine the level of cybersecurity protection commensurate with potential consequences from a cyberattack. The intent of this approach is to ensure that analyses are performed until it is demonstrated that a cyberattack cannot result in the consequences listed in 10 CFR 73.110. This may result in a single tier of analysis being performed, two tiers of analysis being performed (i.e., first and second tier), or all three tiers of analysis being performed. The following sections provide a more detailed explanation of how this three-tier analysis approach is being implemented in the DG.

### Overview of draft regulatory guidance using a performance-based and risk informed approach

The analysis approach discussed herein employs the following two terms:

* CEAS: Cyber-Enabled Accident Scenario, which refers to postulated accidents that are used to assess the potential radiological sabotage consequences resulting from a cyberattack. The CEAS development is risk-informed and leverages the safety-related analysis performed for a given AR design.
* CEIS: Cyber-Enabled Physical Intrusion Scenario, which refers to postulated scenarios that are used to assess the potential unacceptable physical intrusion consequences from a cyberattack. The CEIS assessment allows for insights to implement effective mitigations against cyberattacks to prevent unacceptable physical intrusion consequences.

The analysis approach shown in Fig. 2 through Fig. 4, which is described in the DG, is intended to ensure that only systems that are relied upon or perform functions that can contribute to the 10 CFR 73.110 consequences are assessed and protected.



FIG. 2. Performance-based/risk informed analysis approach – Part 1 [8].

As part of the facility analysis listed in Fig. 2 above, the existing results of safety and security assessments are used to analyze the impact of the loss or compromise of a plant function to determine if it would result in an unacceptable consequence, as defined in 10 CFR 73.110. The focus for this portion of the analysis is to evaluate potential cyberattack consequences considering the plant design basis and physical protection system. CEAS and CEIS, described above, help identify those cyberattack scenarios that have the potential to result in the consequences defined in 10 CFR 73.110 so that they can be protected against.

If a cyberattack results in the consequences defined in 10 CFR 73.110, then enhancements to the AR design and/or physical protection system should be considered, if allowed by a security-by-design approach. A security-by-design approach refers to the consideration of safety and security together in the design process, such that security issues (e.g., newly identified threats of adversary attacks) can be effectively resolved through facility design, engineered security features, and formulation of mitigation measures, with minimal or no reliance on human actions. If a cyberattack does not result in the consequences defined in 10 CFR 73.110, then the operator documents the design basis elements and physical protection system features which ensure that potential cyberattacks do not result in those consequences.

If the preceding analysis shows that a cyber-enabled scenario results in the consequences defined in 10 CFR 73.110 and use of a security-by-design approach is not feasible, then the operator proceeds with the function level analysis (the next tier of analysis) by developing adversary functional scenarios[[3]](#footnote-4) as shown in Fig. 3. This analysis is aimed at managing functional risks. The objective of this analysis is to assess whether and how an adversary can affect the functions via a cyberattack, thus leading to radiological sabotage or physical intrusion scenarios that result in unacceptable consequences. Based on the outcome of the adversary functional scenarios, the operator can manage functional risks by specifying prohibitive cybersecurity plan elements, such as prohibiting the use of wireless technology for certain plant applications or the use of passive/deterministic defensive cybersecurity architecture (DCSA) elements, such as a data diode, to protect against from cyberattacks. The adversary functional scenario analysis helps identify incident scenarios to inform design, development, and implementation of DCSA and other common, facility-wide elements that provide a plant capability (e.g., resilience) that can be leveraged to provide protection against cyberattacks; specifically, those cyberattacks associated with unacceptable consequences as defined in 10 CFR 73.110.



FIG. 3. Performance-based/risk informed analysis approach – Part 2 [8].

If the analysis results reveal that there are any remaining unmitigated adversary functional scenarios and the implementation of passive defense features are not feasible, then the operator proceeds to perform the system level, or the third-tier, analysis as shown in Fig. 4 below. For cases where there are no remaining unmitigated adversary functional scenarios, proceeding with the next tier of analysis would be optional, as operators may decide to do so to increase or further enhance their defense-in-depth posture against cyberattacks. As part of the system level analysis depicted in Fig. 4, the operator needs to identify the critical functions and associated systems via the use of a graded approach. Critical functions are those that are associated with a CEAS or CEIS. Critical systems may be categorized into most critical or least critical, allowing for a graded approach to be applied in the selection and implementation of cybersecurity control measures.



FIG. 4. Performance-based/risk informed analysis approach – Part 3 [8].

Adversary technical sequences are sequences of adversary tactics, techniques, and procedures that the operator should protect against. Frameworks such as MITRE ATT&CK [9] can be used to develop adversary technical sequences that are consistent and reproducible. The outcome of the adversary technical sequences approach helps identify cybersecurity control measures and controls on system design and operation to protect critical function(s) via the application of a graded approach and implementation of defense-in-depth approaches for prevention, detection, and response against cyberattacks. As shown in Fig. 4, this iterative analysis proceeds until all adversary technical sequences are mitigated. Once this objective is achieved, the operator would need to document the cybersecurity plan and DCSA elements, including cybersecurity controls, needed to protect against cyberattacks.

## Novel Design Features and Use Cases

As the NRC prepares to regulate ARs, NRC staff have engaged SMR developers, many of which are proposing the use of technology that is considered novel in comparison to the technology of currently operating power reactors in the U.S. [10]. For example, developers have discussed the use of autonomous operation, remote operation, and remote monitoring. The NRC staff has identified both near-term and longer-term strategies to address these topics. Near-term strategies will enable the NRC staff to address these and other novel technologies under the existing regulatory framework. The longer-term activities focus on options for the NRC staff to engage the Commission on future policy topics for ARs, such as potential licensing and policy related matters for SMRs.

### Regulatory implications

During recent stakeholder interactions with the NRC staff, SMR developers highlighted designs that featured smaller power outputs, passive safety functions, and considerably smaller facility footprints than used for currently operating power reactors; accordingly, the behavior in response to transients and accidents will differ from traditional light water reactors. Several AR developers have also expressed significant interest in the inclusion of autonomous and remote operational characteristics in their proposed designs [10]. Knowledge of these potential design features provided insights to the NRC staff in drafting the proposed 10 CFR Part 53 requirements so that critical digital computer and communication systems and networks are adequately protected against cyberattacks in a manner that is commensurate with the potential consequences of those attacks. Proposed autonomous operation cases seek to eliminate reliance on human interactions, while remote operation and smaller facility footprint cases focus on minimizing the number of operators and other categories of on-site staff. Autonomous operation, remote operation, and remote monitoring raise potential licensing and policy related matters that would require the NRC staff to reassess current requirements as near-term strategies for the use cases and may require exemptions from existing requirements[[4]](#footnote-5).

The requirements in 10 CFR 73.54 apply to operating power reactors and new reactor license applicants and do not specifically address autonomous or remote operations; however, the performance-based nature of the regulation allows for both through application of appropriate cybersecurity measures in an operator’s cybersecurity plan. Under 10 CFR 73.54(a), applicants for an operating license[[5]](#footnote-6) and holders of a combined license[[6]](#footnote-7) are required to address the protection of digital computer and communication systems and networks in their cybersecurity plans. Depending on the level of autonomy, SMR designers could propose using wired, wireless, or a combination of both pathways to establish communications between critical systems and critical digital assets. Data communication pathways that could adversely impact SSEP functions would be within the scope of digital computer and communication systems and networks required to be protected under 10 CFR 73.54(a) against cyberattacks, up to and including the design basis threat.

The level of autonomy [14], remote operations, and remote monitoring are important aspects in understanding the associated cybersecurity risks. A DCSA that incorporates autonomy or remote technology must ensure the confidentiality, integrity, and availability of digital computer and communication systems and networks associated with SSEP functions. Additionally, this architecture would have to be implemented as part of a mutually supportive framework that includes broader physical protection considerations, such as physical security and access authorization. Fully understanding the architecture will be key in providing insights about the attack surface and potential attack vectors. It is likely that protection against disruption or malicious control for SMRs will rely heavily on properly implemented DCSAs. Furthermore, it will be equally important to understand the cybersecurity impacts of the level of autonomy, autonomous tasks, and autonomous technologies used to replace or assist humans for remote operations.

## Future Work

The NRC periodically made the preliminary proposed rule publicly available, sought public comments, and made changes to the proposed rule language in response to stakeholder feedback. The NRC staff are working to address feedback from the NRC’s Commission, with a goal of finalizing the rule along with the implementation guidance by 2027. Key documents related to the 10 CFR Part 53 rulemaking, including preliminary proposed rule language, stakeholder comments, and information related to the schedule are publicly available.

The NRC staff plans to continue working on topics such as the following for inclusion in the DG in support of the draft cybersecurity requirements for ARs: (1) providing guidance for using a performance-based approach for the selection of cybersecurity measures; and (2) providing guidance for the use of emerging technologies such as remote and autonomous operation of reactors. These activities are supported by ongoing research initiatives to inform the staff and establish a better understanding of the cybersecurity considerations associated with the use of emerging technology in nuclear power plants, as well as potential graded and technology-inclusive frameworks associated with the application of these technologies. These research efforts will support finalizing the proposed cybersecurity requirements and DG for inclusion in the proposed 10 CFR Part 53 rule.

ACKNOWLEDGEMENTS

We thank our colleagues from the Department of Energy national laboratories and U.S. universities who provided insight and expertise that greatly assisted during the development of DG-5075, “Establishing Cybersecurity Programs for Commercial Nuclear Plants Licensed Under 10 CFR Part 53” [8], which is a key element of the cybersecurity regulatory framework being developed for ARs. We also thank our NRC staff and management who provided support for the development of this paper.

References[[7]](#footnote-8)

1. U.S. Code of Federal Regulations (CFR), “Physical Protection of Plants and Materials,” Part 73, Chapter 1, Title 10, “Energy.”
2. U.S. CFR, “Requirements for Physical Protection of Licensed Activities in Nuclear Power Reactors Against Radiological Sabotage,” Part 73.55, Chapter 1, Title 10, “Energy.”
3. U.S. CFR, “Protection of Digital Computer and Communication Systems and Networks,” Part 73.54, Chapter 1, Title 10, “Energy.”
4. Cyber Security Programs for Nuclear Power Reactors, Revision 1, Regulatory Guide (RG) 5.71, U.S. Nuclear Regulatory Commission (NRC), Washington, DC, 2023. Available: ADAMS Accession No. ML22258A204
5. “Cyber Security Plan for Nuclear Power Reactors,” NEI 08-09, Nuclear Energy Institute (NEI), Washington, DC, (2010).
6. S.512 - 115th U.S. Congress (2017-2018): Nuclear Energy Innovation and Modernization Act (NEIMA), (2019). Available: https://www.congress.gov/bill/115th-congress/senate-bill/512
7. “Risk-Informed, Technology-Inclusive Regulatory Framework for Advanced Reactors,” Enclosure 1, The Office of the Secretary Paper (SECY)-23-0021, U.S. NRC, Washington, DC, (2024). Available: ADAMS Accession No. ML21162A102
8. “Establishing Cybersecurity Programs for Commercial Nuclear Plants Licensed Under 10 CFR Part 53,” Draft Guidance (DG)-5075, U.S. NRC, Washington, DC, (2024). Available: ADAMS Accession No. ML23286A278
9. MITRE Corporation, MITRE ATT&CK for Industrial Control Systems: Design and Philosophy (2020), <https://attack.mitre.org/>
10. “Micro-Reactor Licensing and Deployment Considerations: Fuel Loading and Operational Testing at a Factory,” Enclosure 1, SECY-24-0008, U.S. NRC, Washington, DC, (2024). Available: ADAMS Accession No. ML23207A252
11. “Policy and Licensing Considerations Related to Micro-Reactors,” SECY-20-0093, U.S. NRC, Washington, DC, (2020). Available: ADAMS Accession No. ML20129J985
12. U.S. CFR, “Domestic Licensing of Production and Utilization Facilities,” Part 50, Chapter 1, Title 10, “Energy.”
13. U.S. CFR, “Licenses, Certifications, and Approvals for Nuclear Power Plants,” Part 52, Chapter 1, Title 10, “Energy.”
14. A. Kim et al., “Cybersecurity Considerations of Autonomy in Nuclear Facilities (Cybersecurity Licensing Activities),” International Conference on Nuclear Security: Shaping the Future, IAEA, Vienna (2024).
1. Information related to the Part 53 rulemaking can be found at Regulations.gov under Docket ID NRC-2019-0062 or <https://www.regulations.gov/docket/NRC-2019-0062>. [↑](#footnote-ref-2)
2. The specific publications can be found referenced in DG-5075 [8]. [↑](#footnote-ref-3)
3. Sequences of adversary accesses to attack pathways that advance CEASs and CEISs through the compromise of functions [8]. These scenarios are based on the threat assessments and reflect the potential effects on facility functions of the compromise of systems performing those functions. These scenarios include those involving radiological sabotage or physical intrusion resulting in unacceptable consequences. [↑](#footnote-ref-4)
4. The licensing and policy related considerations are discussed in detailed in SECY-20-0093, “Policy and Licensing Considerations Related to Micro-Reactors,” [11] and SECY-24-0008, “Micro-Reactor Licensing and Deployment Considerations: Fuel Loading and Operational Testing at a Factory” [10]. [↑](#footnote-ref-5)
5. A two-step licensing process defined in 10 CFR Part 50, “Domestic Licensing of Production and Utilization Facilities” [12] that requires a separate construction permit and operating license. [↑](#footnote-ref-6)
6. An alternative licensing process defined in 10 CFR Part 52, “Licenses, Certifications, and Approvals for Nuclear Power Plants” [13] that combines a construction permit and an operating license with conditions for plant operation into a single combined operating license. [↑](#footnote-ref-7)
7. Publicly available NRC published documents are available electronically through the NRC Library on the NRC’s public website at http://www.nrc.gov/reading-rm/doc-collections/ and through the NRC’s Agencywide Documents Access and Management System (ADAMS) at http://www.nrc.gov/reading-rm/adams.html The documents can also be viewed online or printed for a fee in the NRC’s Public Document Room (PDR) at 11555 Rockville Pike, Rockville, MD. For problems with ADAMS, contact the PDR staff at 301-415-4737 or (800) 397-4209; fax (301) 415-3548; or e-mail pdr.resource@nrc.gov. Documents that are withheld from the public can be requested by those individuals who have established a “need-to-know” and possess access permission to Official Use Only-Security-Related Information (OUO-SRI) or safeguards information (SGI) (or security clearance for classified documents).

Publications from the Nuclear Energy Institute (NEI) are available at its website: http://www.nei.org/ or by contacting the headquarters at Nuclear Energy Institute, 1776 I Street, NW, Washington, DC 20006-3708, at (202) 739-800, or fax (202) 785-4019. [↑](#footnote-ref-8)