INL/CON-24-76665-Revision-0

Risk Analysis for Remote Operation of Microreactors

October 2024

Megan Jordan Culler, Joe Eugene Oncken, Kaeley Renee Stevens, Thomas A Ulrich

Changing the World's Energy Future

Idaho National Laboratory

INL is a U.S. Department of Energy National Laboratory operated by Battelle Energy Alliance, LLC

INL/CON-24-76665-Revision-0

Risk Analysis for Remote Operation of Microreactors

Megan Jordan Culler, Joe Eugene Oncken, Kaeley Renee Stevens, Thomas A Ulrich

October 2024

Idaho National Laboratory
Idaho Falls, Idaho 83415

http://www.inl.gov

Prepared for the
U.S. Department of Energy
Under DOE Idaho Operations Office
Contract DE-AC07-05ID14517

Risk Analysis for Remote Operation of Microreactors

Megan Culler[1,*], Joseph Oncken[1], Kaeley Stevens[1,2], Thomas Ulrich[1]

[1]Idaho National Laboratory, Idaho Falls, ID; [2]Oregan State University, Harrisburg, OR

[leave space for DOI, which will be inserted by ANS]

ABSTRACT

Microreactors are a subset of advanced nuclear reactors that can be factory fabricated, transportable, and self-regulating. They have the potential to be used in microgrids, rural and remote areas, or emergency response applications, replacing fossil fuel sources like diesel generators and enabling sustainable energy generation. In order to make microreactor operation cost-effective, it is likely that remote communications will be needed to reduce the number of personnel required to be on site. While remote operation of energy generation and other industrial control systems is common in other industries, it is not yet adopted in the nuclear community and has many perceived and actual risks. In this paper, the severity of the risks introduced by remote operations for microreactors are explored. The primary changes in the operations involve the addition of a remote communications network and a certification system for data and controls. These changes lend themselves to considerations of cyber risks, whether unintentional or adversarial, but the assessment considers not just cyber risks introduced, but also how physical and human factors-based risks will impact the remote operations system and change the overall risk profile. This initial assessment indicates that there are standard cyber and mitigation measures that can be put in place so the risk of doing remote operations does not dramatically increase compared to local operations. This evaluation is a critical step in the process of evaluating if remote operations of microreactors is a suitable solution to meet future sustainable grid needs.

Keywords: remote operations, nuclear energy, microreactors, risk assessment, cybersecurity

1. INTRODUCTION

In order to meet the White House targets of generating 100% carbon-free electricity by 2035, there will need to be a retirement of coal and natural gas resources and an increase in the deployment of carbon-free resources [1]. While solar, wind, and storage are key components to meet these targets, they may not be sufficient to replace fossil fuel electricity generation and maintain the reliability expected of the grid.

Nuclear energy is a carbon-free option that can help supplement renewable energy and storage and replace coal and natural gas as base-load plants. Large nuclear facilities require arduous processes of approvals and permitting. On top of nuclear safety requirements, they must also navigate transmission queues to add new bulk generation. The nuclear industry is moving towards a new generation of advanced reactors, including microreactors. Microreactors, which generally have a capacity of 20 MW or less, can be used to support distributed energy generation, providing power for remote communities and reliability to critical facilities. They can replace diesel as primary backup resources, and they provide more flexibility in siting, better safety performance, and shorter construction time compared to traditional nuclear plants.

Despite the benefits they provide, key questions remain on how microreactors will be integrated into the grid, whether as part of microgrids with other distributed generators or connected to the grid. In order to be adopted in cost-competitive energy markets, microreactors need to provide energy at reasonable costs and support the stability and reliability of the grid or microgrid by regulating output to balance generation with load and maintain stable voltage and frequency.

Remote operation of microreactors has the potential to lower operating costs by allowing multiple facilities to be managed by one central control center. This will reduce the number of qualified staff necessary to operate microreactors and promote economies of scale by using standardized controls.

Since microreactors are still in early stages of development, it is critical to understand the key, novel risks associated with their development and operations. The need for remote operations in particular presents a novel risk space that has not been addressed in traditional large-scale nuclear generation. Perceived risks include concerns that hackers from across the world could compromise the remote communications, getting access to critical data or even sending malicious commands, or that in the event of physical failures or safety issues with the microreactor, the remote operators would not have enough visibility into the system to properly respond compared to traditional operators that can walk around the plant to physically verify measurements. In this paper, we perform a preliminary all-hazards assessment of the risk introduced by remote operation of microreactors. We focus specifically on the remote operations part of the design, which is a gap in research. We propose key risk mitigations that can be implemented in the design of remote operations using the cyber-informed engineering (CIE) framework, reducing key risks to acceptable levels.

2. BACKGROUND

To understand the risks associated with remote operation of microreactors, we must first understand what microreactors are, how they differ from traditional nuclear generation, why remote operations are needed, and what risk assessment approaches are appropriate to use at this conceptual design phase.

2.1. Microreactor Design

Microreactors are defined as "a subset of [small modular reactors], a category of nuclear reactors designed with smaller capacities required for portability" [2]. Microreactors are intended to be factory fabricated, meaning their components can be manufactured in a facility, then shipped and assembled on site. This reduces difficulties associated with large-scale construction. Due to their small capacities, many microreactor designs will be transportable, making it easier to bring power to where it is needed most. Many designs also include a level of self-regulation, utilizing passive safety systems to reduce the potential for overheating or reactor meltdown. This last point is key in understanding the feasibility of safe remote operations, pointing to the concept that safety operations can be done locally in closed-loop controls, not exposing safety controls to the remote communications platform.

Several manufacturers within the United States are exploring microreactor designs, including General Atomics, NuScale Power, Oklo, Westinghouse, X-Energy, BWXT, and HolosGen [2, 3]. Key considerations for microreactor design include construction materials, fabrication techniques, fuel type, economic viability, environmental impact, and regulatory challenges [2, 4]. Different reactor types may be better suited for different use cases [5]. The U.S. Department of Defense has laid a roadmap for the deployment of the first microreactor by the end of 2027, and the time required from license application to commercial operation is estimated to be seven years [6]. There is still time to develop and commercialize reactor technologies to enable their support of nationwide carbon-free electricity goals, but questions of secure grid integration and operation must be addressed sooner rather than later.

2.2. Grid Integration and Remote Operation of Microreactors

Microreactors have been touted as a flexible, sustainable generation source to supplement renewable generation and replace traditional distributed fossil fuel generation, like diesel generators. However, to take advantage of these benefits, microreactors must have the ability to be operated in conjunction with other resources, whether that is in an isolated microgrid setting or a grid-connected setting. Research has found that microreactors are cost-competitive with diesel generators in microgrid and off-grid applications where

fuel costs are greater than $1.40 per liter [7]. This is an attractive solution in remote areas and microgrids that rely on diesel to provide stability to balance variable renewable energy resources.

Nuclear reactors of any size come with a set of safety and operations challenges. Remote operation microreactors, as required for grid integration, creates a new set of challenges that need to be addressed before this novel technology can be widely deployed. Stevens et. al. describe many of the challenges related to remote microreactor operations, including those related to instrumentation and control, communications, regulatory requirements, human factors, and cybersecurity [8].

2.3. All Hazards Risk Analysis

Since microreactors are still in early phases of development, there have not been many assessments of the risks associated with microreactors, particularly assessments that consider how microreactors will be operated and integrated into the grid. This is a gap that we aim to address.

Existing literature has surveyed the risks associated with microreactors from a regulatory and safety perspective. Operational regulatory analysis has considered primarily the physical design features and the differences between microreactors and traditional light water reactors [9]. Additional regulatory analysis has considered the construction, decommissioning, and transportation strategies for microreactors, and how they differ from traditional nuclear reactors [10]. The transportation analysis must consider the transport of fuel, the transport of in-tact microreactors, and scheduling [11-13]. An example safety analysis of accident scenarios found vulnerabilities related to the moderator material used, the balance of sodium in heat pipes, and the time in which human operators could intervene [14]. These assessments do not cover risks associated with operation and interoperability of microreactors.

2.4. CIE Approach to Risk Mitigation

CIE is a framework supported by the United States Department of Energy that extends "secure-by-design" concepts to the engineering and design of cyber-physical systems [15]. The goal of this approach is to proactively secure digital infrastructure and design systems to be resilient against modern adversaries through mitigation of high consequence risks and consideration of cybersecurity throughout the lifecycle of the system. The remote operations of microreactors is a prime example of a cyber-physical system that must consider the cybersecurity exposure and the physical safety concerns of the system. CIE promotes the opportunity to create cybersecurity improvements in systems through initial design and engineering decisions to reduce the potential for high-consequence outcomes to occur, via natural or adversarial actions. CIE principles include consequence-focused design, engineered controls, secure information architecture, design simplification, layered defense, active defense, interdependency evaluation, digital asset awareness, cyber-secure supply chain controls, planned resilience, engineered information control, and organizational culture. These principles are applied to the proposed remote control architecture to mitigate risks.

3. RISK ASSESSMENT

The risk assessment we perform is a descriptive quantitative analysis, intended to provide comparative analysis for risk prioritization. The purpose is to understand the relative severity of different types of risks, with emphasis on novel risks due to remote operation of microreactors, rather than known risks of traditional nuclear reactor operation. Then, we assess how CIE principles can be applied to mitigate the risks rising from remote operation.

For this assessment, we use the basic calculation of risk as the product of the likelihood and the consequence of the incident under consideration. One of the challenges with risk assessment is that it either requires a high level of specificity about the incident under consideration, assumptions about details describing exactly how the incident occurs and what it effects, or, if more general categories of incidents are evaluated,

there may be a range of likelihoods or consequences for the event, which makes it difficult to quantify. For this high-level assessment, we are examining broad types of events, so in order to provide a level understanding of the comparative risk scores, we define likelihood and consequence each on a scale of 1-5, as described in Table I.

Table I. Likelihood and consequence interpretations for quantitative scoring.

Score	*Likelihood Interpretation*	*Consequence Interpretation*
1	Unlikely to happen ever, but still a possibility	Needs attention, no immediate impact on process control of safety
2	Likely to happen at least once over 10 years of operation	Needs rapid attention, delayed impact to process control or monitoring
3	Likely to happen at least once over 5 years of operation	Requires immediate attention, impacts to remote monitoring and control
4	Likely to happen at least once over 2 years of operation	Remote immediate attention, potential impacts to process functionality
5	Likely to happen at least once within a year	Requires immediate on-site intervention, potential for physical damage or safety impacts

3.1. System Under Consideration

The system that is being assessed is the remote operations and certification system for the remote operation of microreactors, as described in [8, 16]. The proposed system for remote operation includes a remote operations facility, where an operator uses a human machine interface (HMI) to monitor the reactor and send commands. The certification system is designed to ensure that commands sent remotely are safe for the microreactor to implement, to verify that the data at the HMI are accurate, and to provide redundancies in case of failure or malicious injections.

In this proposed remote operations architecture, each command is checked by a digital twin located in the remote operations center (ROC) and a digital twin located at the microreactor to ensure that the proposed command is safe for the reactor to implement. The digital twins provide this guarantee by accurately predicting the future state of the reactor based on the input command and the current known state of the system and checking that the predicted state is safe for the equipment and the grid. A certifier server located at the microreactor receives inputs from both digital twins, and if they agree that the command is safe to execute, the certifier forwards the command to the microreactor control system.

Data verification works in a similar manner. Sensor data are collected, sent to the local digital twin, and transmitted to the ROC digital twin. Each digital twin uses a subset of the sensor data to check that measurements align with what is expected based on the digital twin-predicted states for the microreactor and previous state data collected by a historian. If both digital twins agree that the sensor data align with the expected state of the microreactor, as checked by a certifier server located at the ROC, then the data are displayed on the HMI. If not, the HMI displays an alert, and a debugging process is started to identify the source of the discrepancy.

3.2. Risk Categories

The purpose of this risk assessment is to evaluate major risks associated with the remote operations system and assess whether the proposed system can mitigate these risks. Risk categories were divided into the following subsets:

- Physical system failure (controller and microreactor)
- Remote communications failure
- Remote communications hacking
- Endpoint hacking
- Endpoint failures

Physical system failure includes items such as general and critical sensor failures, sensor drifts, process component failures, and exceeding safety limits. We focus on the impacts of these failures to the remote operations system. For example, a process component breaking may create a situation where the digital twins' models do not agree with the sensor data. Sensor failures may have a similar effect, but a sensor failure may appear as a single anomaly rather than a process level anomaly that is backed by sensor data. The digital twins should diagnose these issues accordingly.

Remote communications failures include network provider outage, router failure, dropped packets, malformed packets, and network throttling. These failures will interfere with the ability to send and receive data in a timely manner, which will have increasing impact as the duration of the failure continues. Loss of remote monitoring and control capabilities creates concerns about the unknown safety state of the microreactor, although as discussed previously, many microreactor designs include closed-loop on-site controls to monitor and react to the safety of the reactor, limiting the risk.

Remote communications hacking covers intentionally malicious activities against the remote communications architecture. Attacks of interest include denial-of-service attacks, man-in-the-middle attacks, replay attacks, and traffic sniffing. The potential for this kind of attack will vary widely based on how the communications architecture is set up. Fiber optic communication lines would have to be physically accessed to be intercepted, while network traffic over the public internet would be much more accessible from around the world. Intermediate solutions, such as the use of dedicated cellular networks, virtual private networks (VPNs), and layered defenses of firewalls, de-militarized zones (DMZs), and other techniques increase the protection of the remote communications while still leveraging wireless technologies.

Endpoint hacking risks include compromise of any of the various computing machines associated with the remote operations system. These include the remote operator workstation, the HMI, the digital twins at the control room and at the microreactor, or the historian. The range of endpoint hacking consequences are large. Simple malware infections could degrade the speed and performance of these machines, while advanced attacks could allow adversaries complete root control over the system. Without diving in to the detail of various attacks that are possible, the focus should remain on the highest consequence associated with the most severe attack on each endpoint.

Lastly, endpoint failures include software failures, bad software updates, bad operating system updates, database failures, and human error. These too have a wide range of potential impact, but bad inputs from a human operator with elevated privileges could have the highest consequence. Risks evaluated in this category focus more on the process layer that is affected rather than which specific machine is affected.

Each risk scenario was evaluated conservatively, meaning that scenarios with ranges of likelihoods and consequences were scored highly to avoid underplaying high risks. The intent is not to authoritatively assign a permanent risk score, but rather to evaluate risks relatively against one another and assess the impact of mitigations on the overall risk profile. The initial, unmitigated risks are shown in Figure 1. No catastrophic (high likelihood, high consequence) events are found, but scenarios are clustered in the higher consequences.

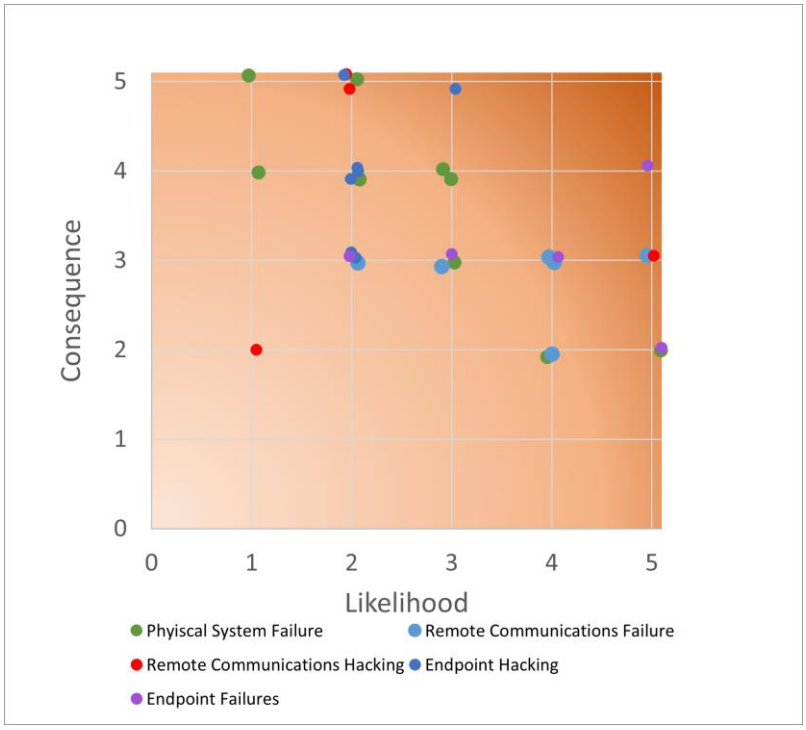

Figure 1. Preliminary risk assessment for remote operations system for microreactors without mitigations. Each dot represents a potential incident that falls within the color-coded risk category. Jitter is applied to make overlapping points visible.

There are both maximum consequence and maximum likelihood scenarios assessed. The lowest overall risk score is a 2, and the highest is a 20, out of a maximum risk score of 25. This assessment supports the perception that there are notable and high risks associated with the proposed remote communications architecture before mitigations are applied.

4. CIE-BASED RISK MITIGATION

The CIE Implementation Guide outlines CIE considerations for each phase of a system's lifecycle to employ these principles [15]. For this analysis, the focus is on the concept, requirements, and design stages of the system. Additional considerations can be added to further mitigate risks in the development, testing and validation, operations and maintenance, and retirement and replacement stages. Each risk was evaluated independently, but we highlight some of the key mitigation actions taken across key CIE principles.

4.1. Application of CIE Principles

Each of the twelve CIE principles are applied at a high level to the proposed remote communications framework to mitigate the identified risks. As remote communications architectures are built and tested, more specific approaches for some of these principles may be required to address the specific physical and digital design decisions made.

The initial assessment lends itself to consideration of consequence-focused design. The key functionality of the microreactor is to maintain nuclear stability and safety. This high consequence has already been engineered out of the remote operations design by allowing resilient, automated, local controls to maintain the safety of the system, using mitigations such as gravitational insertion of control rods and alignment of valves to the safe position if power is lost. For risks introduced by remote operations, the primary

consequences are the loss of remote monitoring or control. Depending on the microreactor application, this could have detrimental effects on the connected power system, such as loss of load or grid stability. Mitigations include items like the use of congestion control algorithms to recover from throttled or dropped data quickly to restore monitoring and control and caching of software backups prior to updates to ensure quick recoveries are made if issues are discovered with the updates.

Engineered controls can be used to eliminate, substitute, and mitigate hazard effects. Threats like cyber adversaries cannot be fully eliminated, but controls can be used to limit their impact to the system. Traffic from unauthorized sources should be dropped, and network segmentation should be implemented to limit exposure to critical endpoints. Only necessary remote functionalities should be designed into the system. Processes that can be done with local control loops limits the attack exposure for the system. Administrative controls can also be applied to ensure that personnel are properly trained on the remote operation system.

A secure information architecture should be designed to prevent undesired manipulation of data. Backups of historians should be saved frequently, and databases can be checked against backups to ensure against tampering. Simple protocol features like checksums can be used for data integrity checks on network traffic, and support encryption and authentication in the protocols selected for network traffic can protect against malicious tampering with the data. Protocols selected should use standardized encryption and authentication methods rather than creating new ones, as custom implementations are often easier to hack.

Design simplification requires consideration of what features are necessary to achieve critical functionality. Although the digital twin certification system adds complexity to the system, the benefits it provides to ensure safe operation of the system and accurate situational awareness for operators are critical. Other mitigations in this area may include removing unused or unnecessary applications and software from workstations and servers in the remote operations system.

Layered defense is a principle to ensure that not only a strong perimeter is built, but that mitigations are set up at each level of the system to limit consequences and make adversarial actions or simultaneous failures across systems more difficult. Multi-factor authentication should be used on operator workstations to ensure that authorized users only have access to critical systems, and additional physical controls should be used at both remote operations sites and microreactor sites. Antivirus software should be deployed on each endpoint, and additional policies should be implemented to reject devices like USBs or other physical connectors by default.

Active defense can include threat monitoring, automated responses to threats, and operator response plans. Intrusion detection systems should be deployed on endpoints. Backup plans for the loss of communications or other cyber events should be developed and practiced.

An interdependency evaluation reveals how the certification architecture is dependent on the sensor information and physical process. A physical system failure may cause inaccurate remote operator view. The certification system is designed to detect and debug these types of issues, but redundant sensors and asset health monitoring can help reduce this risk.

Digital asset awareness requires understanding of where digital assets are used, what functions they are capable of, and what assumptions exist about how they work. The basic remote operations concept limits the computing machines required, but this model could quickly get complex if multiple microreactors are operated from a central ROC, if power grid operators or others require access to monitoring data, or other operational considerations are developed. In addition to these computing assets, designers should be aware of the supporting equipment required, such as switches, firewalls, and protocol converters, that could contribute to a potential attack surface.

Cyber-secure supply chain is a principle important to address not only in the design and vendor selection performed at the start of a project but throughout the lifetime of the project. Software and hardware bills of materials should be developed and maintained, understanding the source of the assets and all their sub-components. Secure updates and patch management strategies may be developed under this principle.

Having a plan for what happens when something goes wrong is a key piece of the planned resilience principle. Consideration of what people, materials, and equipment are needed to withstand a high consequence event, identification of critical system functions, and understanding limits of acceptable performance for critical functions enables adaptation and limitation of consequences when a hazard occurs. Incident response plans for physical and cyber hazards should be developed and tested regularly.

The design principle of engineering information control focuses on managing knowledge about the system. Although security through obscurity is generally not considered a best practice, mission critical information about system operations should be appropriately protected from public view. Role-based access control should be used to limit who has access to what information, and the principle of least privilege should be applied when making information available.

Organizational culture should be intentionally crafted to ensure that all personnel understand the impact of their behaviors and decisions on essential functions. The nuclear industry already has a strong culture of safety, which should be extended to considerations of remote operation.

4.2. Risk Reduction

With the controls applied as described for each of the CIE principles, a re-evaluation of the remote operations system is performed. Primary risk reduction is achieved through consequence reduction, as shown in Figure 2. It is difficult to affect the likelihood of adversary actions or component failures, but attack surface exposure can be reduced, reducing the likelihood of events, and proactive asset health monitoring can help prevent failures.

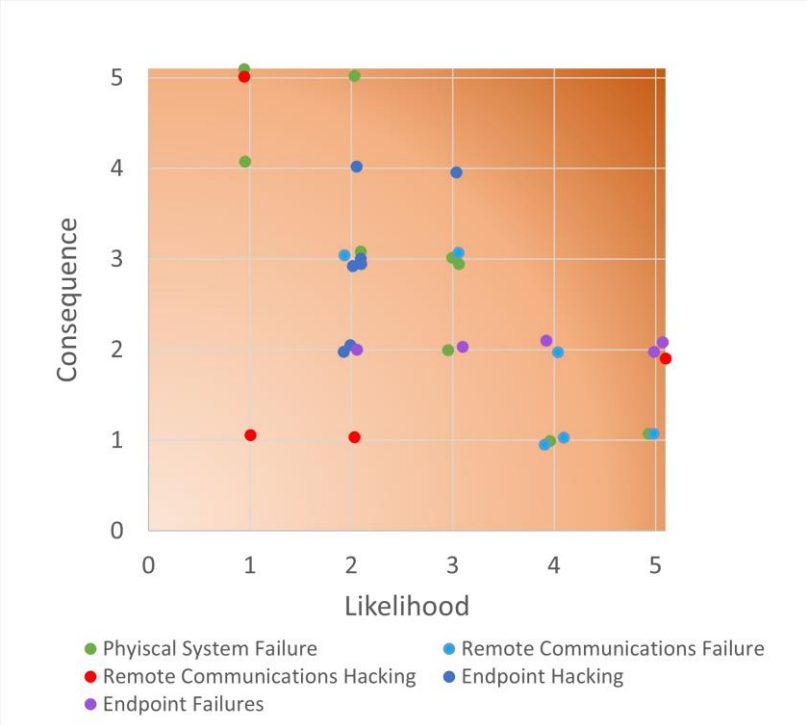

Figure 2. Risk assessment for remote operations system for microreactors with CIE-based mitigations applied to design. Each dot represents a potential incident that falls within the color-coded risk category. Jitter is applied to make overlapping points visible.

There is a notable reduction in the overall risk profile, though high-risk scenarios should be evaluated further to reduce risk to acceptable levels.

Many of the practices described in this mitigation section are standard across business network and industrial system applications. Risk mitigation and security of remote operations for microreactors does not require novel security methods or novel remote communications network architectures. However, since the application space is new and there is high public interest and concern around any nuclear power operations, it is important to ensure that best practices from mature remote communications applications are followed and any unique risks of this application are given proper consideration.

5. CONCLUSIONS

A preliminary all-hazards assessment was performed to evaluate the risks introduced by remote operation in the context of microreactor deployment. Although remote operation for industrial control system assets is not a novel concept, microreactors are a technology still under development, which presents a unique opportunity to ensure that secure, resilient communications are designed to support deployment. Many of the risk mitigation measures suggested are well-known best practices, but they are not all applied across the power industry, and historically, interactions with outdated devices and the need for backwards compatibility has limited implementation of risk mitigations for remote communications. Including these mitigations from the design phase for microreactors will minimize risks from many threat sources. This assessment and simple application of CIE principles demonstrates a reduction in overall risk profile for remote communications that can be achieved with thoughtful consideration of the risks in the design stage.

ACKNOWLEDGMENTS

This work is supported through the Idaho National Laboratory Directed Research & Development Program (LDRD) under Department of Energy Idaho Operations Office contract no. DE-AC07-05ID14517.Neither the U.S. Government, nor any agency thereof, nor any of their employees makes any warranty, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights.

The authors would like to acknowledge contributions from their LDRD team, including Haydn Bryan, Ronald Boring, Stephen Bukowski, Troy Unruh, Dylan Jurski, and Jeren Browning. We also extend our gratitude to the Fission Battery Initiative team for their support of this research.

REFERENCES

[1] (2021). *Executive Order 14008, Tackling the Climate Crisis at Home and Abroad*. [Online] Available: https://www.federalregister.gov/documents/2021/02/01/2021-02177/tackling-the-climate-crisis-at-home-and-abroad

[2] G. Black, D. Shropshire, K. Araújo, and A. van Heek, "Prospects for nuclear microreactors: A review of the technology, economics, and regulatory considerations," *Nuclear Technology,* vol. 209, no. sup1, pp. S1-S20, 2023.

[3] R. Testoni, A. Bersano, and S. Segantin, "Review of nuclear microreactors: Status, potentialities and challenges," *Progress in Nuclear Energy,* vol. 138, p. 103822, 2021.

[4] P. L. Mills, D. J. Quiram, and J. F. Ryley, "Microreactor technology and process miniaturization for catalytic reactions—A perspective on recent developments and emerging technologies," *Chemical Engineering Science,* vol. 62, no. 24, pp. 6992-7010, 2007.

[5] J. C. Kennedy, P. Sabharwall, S. M. Bragg-Sitton, K. L. Frick, P. McClure, and D. Rao, "Special Purpose Application Reactors: Systems Integration Decision Support," Idaho National Lab.(INL), Idaho Falls, ID (United States), 2018.

[6] M. Nichol, "Roadmap for the Deployment of Micro-reactors for US Department of Defense Domestic Installations," *Nuclear Energy Institute, October,* vol. 4, 2018.

[7] J. R. Lovering, "A Techno-Economic Evaluation of Microreactors for Off-Grid and Microgrid Applications," *Sustainable Cities and Society,* vol. 95, p. 104620, 2023.

[8] K. R. Stevens *et al.*, "Opportunities and Challenges for Remote Microreactor Operations," 2023.

[9] D. Owusu, M. R. Holbrook, and P. Sabharwall, "Regulatory and licensing strategy for microreactor technology," Idaho National Lab.(INL), Idaho Falls, ID (United States), 2018.

[10] A. Huning, S. Arndt, and J. A. Christensen, "An Introduction to Microreactor Licensing Basis Events," Oak Ridge National Laboratory (ORNL), Oak Ridge, TN (United States), 2023.

[11] G. A. Coles, S. M. Short, S. J. Maheras, and H. E. Adkins, "Proposed Risk-Informed Regulatory Framework for Approval of Microreactor Transportation Packages," Pacific Northwest National Lab.(PNNL), Richland, WA (United States), 2021.

[12] H. Adkins and S. Maheras, "Microreactor Transportability Challenges–21072," *Pacific Northwest national Laboratory,* 2021.

[13] W. L. Moe, "Key Regulatory Issues in Nuclear Micro-Reactor Transport and Siting," Idaho National Lab.(INL), Idaho Falls, ID (United States), 2019.

[14] F. Antonello, J. Buongiorno, and E. Zio, "Insights in the safety analysis of an early microreactor design," *Nuclear Engineering and Design,* vol. 404, p. 112203, 2023.

[15] "National Cyber-Informed Engineering Strategy from the U.S. Department of Energy," *U.S. Department of Energy (DOE) Office of Cybersecurity, Energy Security, and Emergency Response (CESER)*, June 2022.

[16] T. Ulrich *et al.*, "Digital Twin Verification for Advanced Reactor Remote Operations," in *Accelerating Open Access Science in Human Factors Engineering and Human-Centered Computing*, 2023: AHFE International, doi: 10.54941/ahfe1003551. [Online]. Available: https://openaccess.cms-conferences.org/publications/book/978-1-958651-58-2/article/978-1-958651-58-2_3

[17] V. Wright *et al.,* "Cyber-Informed Engineering Implementation Guide," Idaho National Lab. (INL), Idaho Falls, ID (United States), 2023.