INL/CON-22-70150-Revision-1

# Opportunities and Challenges for Remote Microreactor Operations

July 2023

Kaeley Renee Stevens, Joseph Eugene Oncken, Haydn C Bryan, Izabela Gutowska, Thomas A Ulrich, Ronald Laurids Boring PhD, Megan Jordan Culler

## DISCLAIMER

This information was prepared as an account of work sponsored by an agency of the U.S. Government. Neither the U.S. Government nor any agency thereof, nor any of their employees, makes any warranty, expressed or implied, 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. References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the U.S. Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the U.S. Government or any agency thereof.

INL/CON-22-70150-Revision-1

# Opportunities and Challenges for Remote Microreactor Operations

**Kaeley Renee Stevens, Joseph Eugene Oncken, Haydn C Bryan, Izabela Gutowska, Thomas A Ulrich, Ronald Laurids Boring PhD, Megan Jordan Culler**

**July 2023**

**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**

# Opportunities and Challenges for Remote Microreactor Operations

**Kaeley Stevens[1], Joseph Oncken[1], Ronald Boring[1], Thomas Ulrich[1], Haydn Bryan[1], Megan Culler[1], Izabela Gutowska[2]**

[1]Idaho National Laboratory, Idaho Falls, ID
[2]Oregon State University, Corvallis, OR

## ABSTRACT

The nuclear industry is developing new advanced reactor technologies, and many companies are embracing this advancement by pursuing the development of microreactors. The term microreactor generally refers to a nuclear reactor with an operating power of 20 MW or less. The power range of microreactors makes them appealing for many use cases, such as powering remote communities, mining sites, and military bases. Most of the microreactor designs being pursued will incorporate remote facility operations into the final product. However, no framework has yet been developed to determine what remote operations systems require for reliable, resilient, and secure operation of a microreactor.

This work identifies the challenges unique to remote operations and monitoring for microreactors specifically regarding instrumentation and control, communication methods, regulatory requirements, and operational policies. The types of commands and sensor measurements that must be transmitted between the facilities as well as methods for verifying the trustworthiness of these signals are assessed. This work evaluates the security, reliability, and performance requirements that must be met when considering the selection of communication hardware and protocols for use in remote operations. Also, an assessment was performed to study how remote operations fit within current regulatory requirements and what may need to be updated in regulatory policy to allow for remote operation. Finally, the operational contingencies unique to remote operations that must be in place for response to abnormal events are identified. This paper details these challenges and research opportunities to provide a foundation for the design of remote operation systems.

*Key Words*: microreactor, remote operation, digital twin

## 1. INTRODUCTION

Microreactors are “a subset of [small modular reactors], a category of nuclear reactors designed with smaller capacities required for portability” [1], generally with an operating power of 20 MW or less. Various microreactor designs are being explored internationally, as well as within the United States. Some developers of microreactor designs being developed in the U.S. are: General Atomics, NuScale Power, Oklo, Westinghouse, and X-Energy [1]. The small size of these microreactors makes them useful for many different applications for which large-scale plants would not be suitable. For instance, they can be used for powering remote communities, mining sites, military bases, and ship propulsion. Most of those applications currently rely on diesel generators for power and replacing those generators with carbon-free energy (with a microreactor on its own, or by pairing solar/wind with a microreactor) is the key benefit of microreactor development.

Microreactors are being considered for use in remote locations, which introduces a unique set of challenges. There is uncertainty concerning development costs, undefined licensing requirements, and the ability of microreactors to be cost competitive [2]. Microreactor designs are still in development, and many of the designs are planning to use features that are different from those in currently operating commercial plants. These technologies are not proven and have no operating experience in the U.S., which drives up the cost. That combined with the significantly smaller amount of power being produced by a microreactor leads to questions about the economics of producing microreactors. Implementing remote operation for microreactors has the potential to greatly improve the economics of the facility. However, many planned applications of microreactors are remote, so it may be difficult to find the number of qualified staff that would be necessary for on-site operation. A semi-autonomous remote operating system could allow for operation from a more centralized location while also reducing the number of staff necessary. It could even be possible to operate and monitor multiple microreactor sites from one centrally located remote operating center. Other industries have used remote monitoring and operation from a centralized location including oil and gas facilities [3], wind turbines [4], and mining sites [5]. These applications show that remote monitoring and operation have been done before, and the same concept can be applied to nuclear power.

While remote operation applications for other industries do exist, it has not been done in the nuclear industry and there are heightened safety concerns for the nuclear applications. Remote operation of microreactors has the potential to be very economical and may even be essential for microreactors to be cost-competitive. This paper aims to identify the different challenges and research opportunities that exist in the remote operation and monitoring space. It is part of a larger body of work being performed at Idaho National Laboratory (INL) whose purpose is to create a framework for the resilient and secure remote monitoring and operation of microreactors.

## 2. OPPORTUNITIES FOR REMOTE MICROREACTOR OPERATIONS

As discussed in the previous section, remote operation and control of microreactors is crucial for the successful application of microreactor technology. The small size of these microreactors makes them useful for many different applications for which large-scale plants would not be suitable and reliable base-line power is still needed, but most of those use cases are in remote locations. Semi-autonomous remote operation may be necessary for microreactors to be economically feasible. This section discusses the potential economic effects of remote operation capabilities and the opportunities this presents to increase the technology's adoption rate.

The first commercial adopters of nuclear microreactors are expected to be niche applications with specific technological constraints or high cost next-best alternatives. An example of a relevant remotely operated microreactor first-adopter case is a mining operation in an isolated Arctic area. From an operational standpoint, mining operations require fairly steady energy input because they have high sensitivity to generation reliability. These technological characteristics are expected to be met by microreactors, making them a natural competitor for consideration in this scenario. From an economic standpoint, construction and operational costs tend to be higher in remote areas given transportation, logistical, and labor costs. Remote operation of microreactors can reduce construction costs (no need to build a complete control system onsite) and labor costs (many microreactors could be operated simultaneously from a centralized hub in an area with lower labor costs).

Early adoption of any technology is critical for its continued success in the commercial space. For example, economies of learning reduce the cost of manufacturing, distributing, and operating microreactors – a process that is accelerated when adoption rates are higher. Remotely operated reactors could benefit even more from increased adoption due to significant potential reductions in labor costs. If allowed under regulatory constraints, many reactors could be remotely operated from the same command center, allowing for cumulative economies of scale: fewer full-time equivalents (FTEs) per MWe capacity managed, or per reactor managed. These labor cost reductions could come from the operation staff (one team simultaneously managing multiple reactors) or from reduction of overhead costs.

As microreactors transition from the research and development stage to the commercial market, it is critical that their costs are equal to or lower than those of their alternatives. Remote operation capabilities, as enabled by digital twin technology, may stand as a make-or-break factor for microreactor economic competitiveness for early adopters. In turn, the cost reductions experienced through the accumulation of remotely operated capacity and economies of learning may represent another make-or-break point for wider adoption of the technology. As such, digital twin research is important and potentially critical for the widespread adoption of microreactor technologies.

## 3. CHALLENGES OF REMOTE MICROREACTOR OPERATIONS

There are many factors that need to be addressed in the development of a system for the remote operation of a nuclear reactor. This paper identifies the challenges involved with remote operations specifically regarding instrumentation and control (I&C), communication, regulations, and human factors.

### 3.1 Instrumentation and Control

Many questions will need answers in order to align the I&C systems with the concept of remote operations. What sensor measurements are necessary for operation? What level of autonomy is desired for the system? How can the signals and commands being sent back and forth between the remote operation center and reactor site be trusted? Defining the I&C setup is the initial step to develop a remote operation system framework.

Not all remote operation systems will have the same I&C system needs; each microreactor use case will influence what is necessary. A remote operation system for a microreactor intended to power a mining site may have different sensor needs to obtain the necessary information for operation compared to a microreactor powering a hospital, for instance. Identifying what the microreactor will be used for and ensuring that the remote operations system has the right set of measurements and controls for the specific application are essential primary steps in developing the remote operation system.

Another feature of the remote operation system that is essential in determining the I&C system that is necessary would be the level of automation that is desired for the system. Ramuhalli and Cetiner discussed many concepts for autonomous operation [6], such as the various requirements, concepts, and potential approaches for autonomous microreactor operation. A key concept for these operation systems is the degree of automation. Increased autonomy of operation increases the potential for machine error but reduces the need for human intervention. It is important to find an ideal level of autonomy for the remote operation system when considering the trade-offs involving reduced staffing, system complexity, operational flexibility, etc. [6]. One of the most well-known scales for system automation was defined by Sheridan [7]. His proposed scale has 10 levels of automation, with level 1 being full operator control and level 10 giving the computer complete control. Sheridan’s levels of automation are very general, and many industries have proposed revised perspectives for automation specific to their fields of interest. Additionally, there has been work that focuses on proposing automation levels for nuclear reactor operations by illustrating how industries such as automotive and aerospace have revised and defined their automation levels [8].

The U.S. Nuclear Regulatory Commission (NRC) provides guidelines for automation in reactor operations in Section 9 of NUREG-0700 [9]. However, it has been proposed that if only those guidelines were considered, they would not “align with long-term economic and commercial goals of the advanced reactor community” [8]. It was found that the automation levels defined in Section 9 of NUREG-0700 relied on humans to monitor performance and intervene when needed. With that being the basis for the NUREG guidelines, the automation systems provide operator support rather than replacing operator duties in terms of day-to-day control. Therefore, the knowledge of the automation approaches used in other industries was used to propose revised automation levels that build upon the existing NUREG guidelines while keeping in mind the current nuclear safety standards [8]. The proposed automation levels for nuclear reactors are shown in Table I.

**Table I. Proposed levels of automation for nuclear reactor operations [8]**

| | Level | Human/Machine Interoperability |
|---|---|---|
| 0 | No Automation | Manual control: the operator makes all decisions and performs all actions |
| 1 | Operator Assistance | Operator sets the desired state for a given component. The automated system maintains the given state until directed otherwise. |
| 2 | Automation by Consent | Operator defines optimal conditions for a system of multiple components. The automated system operates within the conditions. The system is closely monitored by operators; they approve actions when requested, provide fallback, and can intervene with commands. |
| 3 | Automation by Exception | Automated reactor operation system (AROS) performs tactical and operational tasks in specific and limited operational domains. Upon request, an operator must approve tactical and operational decisions and provide fallback |
| 4 | High Automation | AROS provides sustained operational and tactical control and fallback in semi-limited operational domains. A fallback-ready reactor supervisor familiar with AROS is required on-site. |
| 5 | Full Automation | AROS provides sustained operational and tactical control and fallback in all operational domains:<br>One-way communication: remote reactor supervisor monitors operations<br>Two-way communication: remote reactor supervisor monitors operations and provides strategic commands as necessary |

Autonomy is appealing because it has the potential to greatly reduce the amount of staff necessary to operate and monitor the reactor, which is an economic benefit that can make the cost of a microreactor more competitive with other options. However, greater autonomy leads to more complexity in the system itself and the hardware necessary to create it.

Autonomous control can be implemented using digital twins. The ongoing digital transformation and implementation of digital twins have led to methods and tool development that can enable the remote operation of microreactors. Digital twins have the capacity for component monitoring and simulating what a command will do before it is sent. These features are crucial for autonomy within a remote operation system. The digital twin concept was first introduced by Michael Grieves at the University of Michigan in 2003, in his product lifecycle management course. Grieves's preliminary digital twin concept was defined as having three components a physical product, a virtual product, and the connections for information transfer between the physical and virtual products to tie them together [10]. The digital twin concept is still in relatively early phases, and it does not yet have a clear, universal use framework, protocol, or definition. Liu, et al. provided an overall review of digital twins and have a lengthy table showing the various definitions of a digital twin within academic publications [11]. Digital twins were initially used mostly by the aerospace industry [11,12]. More industries such as manufacturing, energy, engineering construction, healthcare, agriculture, etc. [12] are beginning to incorporate the use of digital twins. A digital twin can be used for real-time monitoring, system operation and control, and even predictive performance [11]. A semi-autonomous remote operation system will need to utilize digital twins to perform the operation and monitoring functions of the physical system.

Uncertainty about which autonomous control levels are ideal is a significant obstacle for the remote operation system. What commands can the system send on its own? How detailed should those commands be? Advanced reactor designs are incorporating more passive safety features so operator intervention is not always required in emergencies and a core meltdown is prevented by those passive safety features. Is it even necessary for the remote operation system to be capable of an emergency shutdown of the reactor? Initial requirements for full autonomous operation have been proposed [6] and fully autonomous control is the most likely end goal for systems such as this. However, since the remote operation of a reactor has not been implemented yet, a remote operation system should initially focus on incorporating a lower level of autonomy for the system.

Defining the system's autonomous control levels will help identify the necessary sensor measurements to be transmitted from the reactor to the remote operation system. When transmitting sensor data from the reactor facility to the remote operation center there must be a system in place to verify the trustworthiness of the signals and commands. Verification in the context of the remote operation system indicates that the commands and measurements have their integrity preserved – meaning they were not modified in any way – and/or that authentication is preserved, confirming that the data received is sent by the expected sender. The verification system would also need to identify if there is drift or failure of a sensor. Higher levels of autonomy (more detailed commands) would lead to a more complex verification system. The amount of information that needs to be transmitted between facilities directly impacts the necessary communication network for the remote operation system.

### 3.2 Communication Methods

Many of the communication system decisions will depend on the ongoing development of the I&C system. Fortunately, there are multiple communication methods capable of meeting the requirements for latency, bandwidth, channels, availability, and standby. Power systems have long relied on many communication methods (wired, cellular, radio, voice, and satellite) to serve different aspects of coordination for the system. One or multiple of these methods will likely be used for the remote operation of microreactors. Is one method better than the other? The answer relies on the information being sent between the remote operation center and the reactor site. For example, microreactors are expected to provide relatively constant power with moderate ramping rates, which means delays of a few milliseconds or even seconds for power output commands would not drastically impact functionality. However, in the event of an emergency, it is desirable to send emergency shutoff commands as quickly as possible and ensure that the remote operators can have a full view of the situation at the microreactor. This could drive requirements for three or more primary communications channels: control (normal operation), safety, and monitoring. The decisions made for the transmitted measurements and commands must be clearly defined before the best fit for communication hardware can be selected. The aim for a remote operation system is not to create novel communications hardware or networks, therefore commercially available communication hardware (ethernet, I/O, fiber optics, satellites, etc.) will be implemented into its design.

Industrial control systems (ICSs) are the most critical components of any infrastructure, as they collect information from the sensors and field devices, process and display the information, transmit it over the network and send the command communications [13]. The remote operation system is a remotely operated ICS. The system monitors the reactor and has the capacity to send commands, and the interruption in standard remote operation could create power imbalances in the local system leading to grid instability or collapse – the system needs to be secured. This security could involve encryption, authentication, and non-repudiation of transmitted information using NIST-approved cryptographic algorithms. In addition to using standard network security practices, digital twin technology can be used to validate that the sensor data received matches the expected measurements and the received commands do not jeopardize safe operation of the system. Cyber informed engineering (CIE) is a design framework used by INL and adopted by the Department of Energy (DOE) that will be implemented to protect the communications between the remote operations station and the reactor site. CIE is a methodology used throughout the design lifecycle to “characterize the risks presented by the introduction of digital computer systems in a traditionally analog environment and offer a strategy to apply engineering risk processes to mitigate these risks” [14]. This ensures that cyber risks and their minimization are considered from the beginning of the design phase. The CIE method considers the entire system, not just the communication network, meaning the physical and cyber protection of the remote operations center will be an important focus in addition to securing the communication network.

The I&C choices determine the information that is being sent to and from the remote operating center. These decisions will not only influence what communication methods are used, but also what level of cyber security is needed. The communication network and security of the remote operation system will undoubtedly be major considerations in any future remote operation regulatory requirements.

## 3.3 Regulatory Requirements

Section 9 of NUREG-0700 has automation system guidelines for nuclear reactors. The document states that the role of automation extends to “supporting operator decision making and managing the human-system interfaces” [9]. The guidelines for automation review are divided into many subsections, some of which are: automation displays, interaction and control, automation levels, and computerized operator support systems. As it was previously mentioned, the guidelines established in NUREG-0700 use automation as a support for operators rather than a method for replacing some operator duties [8]. That is why revised levels that build upon the NUREG guidelines and incorporate truly autonomous operations for nuclear reactors have been proposed. The intent was to provide a perspective on automation for nuclear reactors that would align with the long-term goals of the advanced reactor community and retain the safety standards that NUREG-0700 provides [8].

While the NRC has provided some guidelines on automation systems, there are no regulations defined for nuclear reactor remote operation. Therefore, one purpose of designing a remote operation system is to develop best practices to help inform the formation of future regulations regarding remote operation. The NRC has released a document detailing the results of a project to identify some ground rules for the feasibility of remote operation regulations [15]. This document includes multiple focus areas that are used to help identify the “ground rules” and “key attributes” that would need to be considered for feasible remote operations of a nuclear reactor. The relationship between the focus areas, ground rules, and key attributes is depicted in Figure 1.

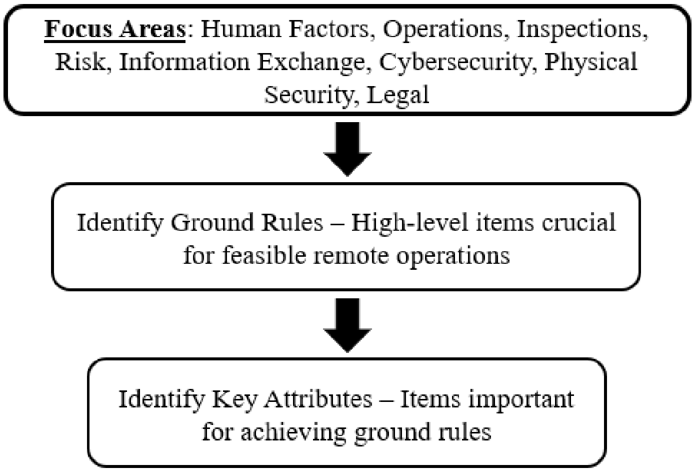
Focus Areas: Human Factors, Operations, Inspections, Risk, Information Exchange, Cybersecurity, Physical Security, Legal
Identify Ground Rules – High-level items crucial for feasible remote operations
Identify Key Attributes – Items important for achieving ground rules

**Figure 1. Relationship between focus areas, ground rules, and key attributes [15]**

With input from subject matter experts, the NRC developed a list of eleven ground rules that detail the main considerations for the implementation of remote operation [15]. Many of these ground rules line up with the challenges the current project plans to address. For instance, one of the ground rules states the importance of considering data and voice communication infrastructure and security from the beginning of development for a remote operation system. A few of the ground rules focus on the need to address the various human factors considerations that will be different for a remote operation system as well. The next section details what this project aims to focus on regarding the human considerations of remote operations.

There is still a lot of work to be done to fully develop regulations for a remote operations system for a nuclear reactor. It is intended that this work will help identify what aspects of remote operations are most important for regulations to focus on as well as any additional considerations that have not yet been addressed by the NRC.

## 3.4 Human Factors Considerations

Determining the automation level for a remote operation system for a microreactor also entails deciding what level of control is appropriate for the operator. Each level of automation has different human factors issues that may arise. Fleming et al. address the key insights regarding human considerations when automating microreactors [16]. Their report identifies and describes issues concerning reduced staffing, assessments of current NRC licensing requirements for nuclear power plants, overviews of current microreactor designs to show how human factors engineering and NRC guidelines may be incorporated and proposing a regulatory approach to review the impacts of reduced staffing [16].

Initially, remotely operated systems will not operate under fully autonomous control of a microreactor. To determine system requirements, it is necessary to consider what tasks are intended to be performed by the human operators [16]. For an early-adoption remote operation system, it should have a heavier emphasis on autonomous monitoring, more so than autonomous control. The limited set of autonomous control actions would take general functional level input from the human operator, the specifics of the control action would be autonomously determined by the system (e.g., an operator command would be to reduce the power level, and from that the system would issue a command that autonomously sets the control drum position to obtain the reduced power level). Having a very limited set of autonomous commands in initial remote operation systems should have fewer human factors considerations to address than a highly autonomous system.

In addition to the level of autonomation for the system and what role the human has within the system, the staffing numbers and qualifications needed for operators of the remote operation system needs to be addressed. The operator responsibilities for a semi-autonomous remotely operated system would be very different from an on-site operator for the current commercial nuclear power plants. The training necessary for remote operators would not be the same for the current on-site operators. Title 10 Code of Federal Regulations (CFR) contains all of the requirements for operators of nuclear facilities. 10 CFR 50.54 details the on-site staffing requirements for nuclear power plants, but it does not address staffing for remote operation scenarios. The changes to staffing requirements and qualifications are serious issues that need to be considered early in the design process of the remote operation system. The NRC has yet to release explicit regulatory guidance to address remote operator requirements, but they have provided public statements that they are intending to update requirements appropriate to the changes in the operators' role for remote systems.

The staffing numbers and training requirements for the operators of the remote operation system also depend on how many microreactors are being operated from a single remote operations site. Having multiple microreactors collectively managed by one remote facility would be the most economical and efficient method for implementing remote operations for microreactors. The number of microreactors per plant and number of plants operated from a single, centralized facility would heavily influence the number of operators needed and how those operators are trained.

The remote operation of a nuclear reactor has not been explored yet. So, there are many human factors challenges – such as, operator role in the system, remote site staffing, education/workforce development, and aggregation of control facilities – that need to be addressed in the implementation of a remote operation system for microreactors. Concepts of operations (ConOps) for advanced reactors are still under development. Remote operations and monitoring, including potential concepts of monitoring (ConMon), remain an important area for research to establish best safety practices.

## 4. CONCLUSIONS AND FUTURE STEPS

Microreactors have the potential to greatly benefit the efforts to reduce carbon emissions. Remote operation is crucial for the implementation of microreactors. A remote operating system will improve the economic feasibility of applying microreactors to their desired uses in isolated locations. However, without any reactors currently operating via a remote command center, there are challenges that must be addressed. Some of the greatest challenges for implementing a remote operation system stem from I&C, communication methods, human factors, and lack of existing regulations. Future work by this team will develop a resilient framework for remote operation while addressing these various challenges.

Future work will include designing a remote operation system for a non-nuclear test facility and utilizing CIE throughout the development to establish a framework applicable for remote operations of microreactors. CIE will ensure that the system is created with physical and cyber security in mind. Digital twins will be used for monitoring, control, and forecasting of the reactor operating state. A verification system is being developed to ensure the trustworthiness of the commands and sensor data being exchanged between the remote center and reactor site. With trustworthy signals and a secure communication network in place, simulations of the remote operation system will be run to test its functionality. Testing will include operation under normal conditions, sensor failures, cyber threats, and more. There will also be a detailed economic assessment for the system.

## ACKNOWLEDGMENTS

The authors would like to acknowledge the support of Troy Unruh, Stephen Bukowski, and Jeren Browning for this paper. 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. The U.S. Government and the publisher, by accepting the article for publication, acknowledges that the U.S. Government retains a nonexclusive, paid-up, irrevocable, worldwide license to publish or reproduce the published form of this manuscript, or allow others to do so, for U.S. Government purposes. Neither the U.S. Government, nor any agency thereof, nor any of their employees makes any warranty, express or implied, 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.

## REFERENCES

1. G. Black, D. Shropshire, K. Araújo, A. van Heek, "Prospects for Nuclear Microreactors: A Review of the Technology, Economics, and Regulatory Considerations," *Nuclear Technology*, **209**, pp.1-20 (2022).
2. R. Testoni, A. Bersano, S. Segantin, "Review of Nuclear Microreactors: Status, Potentialities and Challenges," *Progress in Nuclear Energy*, **138**, pp.1-10 (2021).

3. V. Hepsø and E. Monteiro, "From Integrated Operations to Remote Operations: Socio-technical Challenge for the Oil and Gas Business," *Proceedings of the 21st Congress of the International Ergonomics Association (IEA)*, Vol. 219, pp.169-176 (2021).

4. "Remote Monitoring of Wind Turbine Power Generators," https://www.netbiter.com/applications/applications-leg/wind-power-monitoring#:~:text=A%20Netbiter%20communication%20gateway%20connects,and%20from%20the%20Argos%20server. (2022), accessed February 15, 2023.

5. "Mine Asset Monitoring," https://www.monicoinc.com/industry-monitoring-solutions/mine-monitoring (2021), accessed February 15, 2023.

6. P. Ramuhalli and S.M. Cetiner, "Concepts for Autonomous Operation of Microreactors," *Oak Ridge National Laboratory Report*, pp.1-21 (2019).

7. T.B. Sheridan, *Humans and Automation: System Design and Research Issues*, Wiley, Hoboken United States (2002).

8. A. Alberti, V. Agarwal, I. Gutowska, C. Palmer, C. de Oliveira, "Automation Levels for Nuclear Reactor Operations: A Revised Perspective," *Progress in Nuclear Energy*, **157**, pp.1-12 (2022).

9. J. O'Hara and S. Fleger, *Human-System Interface Design Review Guidelines*, NUREG-0700 Rev. 3 Brookhaven National Lab (BNL), Upton, NY, United States (2020).

10. M. Grieves, "Manufacturing Excellence through Virtual Factory Replication," *Whitepaper*, pp.1-7 (2014).

11. M. Liu, S. Fang, H. Dong, C. Xu, "Review of Digital Twin about Concepts, Technologies, and Industrial Applications," *Journal of Manufacturing Systems*, **58**, pp.346-361 (2021).

12. F. Tao, B. Xiao, Q. Qi, J. Cheng, P. Ji, "Digital Twin Modeling," *Journal of Manufacturing Systems*, **64**, pp.372-389 (2022).

13. R. Masood, "Assessment of Cyber Security Challenges in Nuclear Power Plants Security Incidents, Threats, and Initiatives," *Cyber Security and Privacy Research Institute – The George Washington University*, pp.1-40 (2016).

14. U.S. Department of Energy, "National Cyber-Informed Engineering Strategy," *Final Report*, pp.1-37 (2022).

15. U.S. Nuclear Regulatory Commission, "Grounds Rules for Regulatory Feasibility of Remote Operations of Nuclear Power Plants," *Draft Report*, pp.1-17 (no date).

16. E. Fleming, M. Nyre-Yu, D. Luxat, "Human Factors Considerations for Automating Microreactors," *Sandia National Laboratories Report*, pp.1-64 (2020).