Emerging Technologies and Future of Work, Vol. 117, 2023, 10–20
https://doi.org/10.54941/ahfe1004400

Digital Twin Framework for the Resilient Remote Monitoring and Operation of Nuclear Microreactors

Kaeley Stevens[1], Joseph Oncken[1], Megan Culler[1], Thomas Ulrich[1], Ronald Boring[1], Stephen Bukowski[1], and Izabela Gutowska[2]

[1]Idaho National Laboratory, Idaho Falls, ID 83415, USA
[2]Oregon State University, Corvallis, OR 97333, USA

ABSTRACT

The nuclear industry is developing new advanced reactor technologies, and many companies are conceptualizing designs for microreactors, a class of nuclear reactor with a sub-20 MWth power output designed to be factory fabricated, easily transportable, and simple to control. Microreactors offer promising solutions to several use cases for which large-scale plants would not be suitable, and conventional power generation means, notably diesel electric generators, are expensive and logistically difficult. Many of the potential use cases are in isolated locations such as arctic communities, remote mines, and military installations. Therefore, the cost of microreactor deployment and traditional onsite operations pose a challenge that requires new technical solutions to address. One solution that has the potential to greatly improve economics is to operate and monitor microreactors remotely from a centralized location. Remote monitoring and operation are novel concepts to the nuclear industry and will greatly alter the tasks and responsibilities associated with current commercial nuclear power plant operators. As such, it is important to perform research on potential technological solutions and the impacts those solutions have on operations with end-goal of defining a safe and effective remote concept of operations. This paper proposes a framework for resilient remote operation of microreactors enabled by a novel digital twin implementation.

Keywords: Digital twin, Remote operation, Microreactor

INTRODUCTION

Microreactors are a subset of advanced reactors defined by a capacity of 20 MWth or less. The minimal size provides flexibility in both deployment and operation, which renders them ideal for many cases unsuitable to large-scale reactors, such as powering remote communities, mining sites, and military bases. Many of these applications currently rely on green-house gases producing generators while microreactors can provide carbon-free energy. Microreactors have the potential to address the needs of diverse energy markets; this concept has garnered rapidly growing interest evidenced by numerous competing designs from General Atomics, NuScale Power, Oklo, Westinghouse, and X-Energy (Black et al., 2022).

To realize the great microreactor potential, numerous challenges pertaining to the deployment and operating costs must be addressed. Most microreactor designs will incorporate features that leverage advanced technologies coupled to dramatically different operations than those found at current commercial nuclear power plants (e.g., higher levels of automation resulting in reduced staffing requirements). Since the United States has little to no experience with advanced reactor concepts intended for microreactors, the cost of the initial wave of deployments can be substantial. That, combined with the significantly smaller amount of power being produced by a microreactor, leads to questions about the economic feasibility of deploying microreactors under the same assumptions governing existing reactors' concepts of operations. Operating the microreactor remotely has the potential to greatly improve the economics. A remote operations system affords human oversight from a centralized location and a significant reduction in the number of required staff. High levels of centralization supporting larger groups of multiple microreactor sites may potentially provide the greatest value proposition for their widespread adoption. Other critical infrastructure industries, such as oil and gas (Hepsø and Monteiro, 2021), have mature distributed control system implementations that provide critical knowledge and experience for remote monitoring and operation from a centralized location. Corresponding to the smaller capacity size of the microreactors are other distributed energy resources (DER) that are deployed on the grid for electrical energy production, such as wind, solar, storage, and hybrid plants. These facilities are operated remotely, generally by a centralized operation system with multiple plants throughout the United States and the world. These other industries prove the feasibility of the concept and provide technologies that may prove applicable to nuclear power use cases.

The nuclear power source places higher safety and security concerns on microreactors than other traditional power generators. From a cybersecurity perspective, it is crucial for a remote operations system for nuclear systems be capable of ensuring unauthorized individuals cannot send or alter commands, bad actors cannot modify or block signal transmissions, and the risk of operators receiving or interpreting and then acting on incorrect information to the detriment of the system is prevented. Any remote operation system for a nuclear application will need to be proven safe, resilient, and secure. Since remote operations for nuclear reactors is a nascent concept, we have the duty and opportunity to ensure cybersecurity and resilient communications are considered during early design activities. This can be achieved through the use of cyber-informed engineering (CIE). CIE is a methodology used to implement cybersecurity considerations throughout the entire design life cycle of a system (U.S. Department of Energy, 2022). It allows for cyber risks to be addressed and mitigated or potentially even eliminated early in the design phase. By combining cybersecurity and physical verification processes, we can build a robust layered defense to fulfill this goal.

In addition to a CIE approach, this paper proposes a novel framework for a digital twin-based certification system (DTCS) used in conjunction with a state-of-the-art, secure communication infrastructure to provide an additional layer of security and assurance of the status of the microreactor

as viewed by a remote operator. The DTCS introduces a novel concept of multiple independent verifications of state change over time, producing a significant step toward depth of defense for remote operations. This framework significantly raises the bar to mitigate unauthorized, unsafe, and unallowable commands as well as increase the trustworthiness of the system state information, such as sensor data or component status, sent from the microreactor to the remote operations center.

DIGITAL TWIN-BASED VERIFICATION & VALIDATION SYSTEM FRAMEWORK

The concept of a digital twin was initially introduced by Michael Grieves (2014) and has since then developed with the ongoing implementation of digital twins across many different industries. A digital twin is a virtual representation of a physical system or asset and can be used for real-time monitoring, system operation and control, and even predictive performance or maintenance (Liu et al., 2021). These features allow a DTCS to provide security as well as the ability to diagnose problems.

Trusting that the transmitted sensor measurements and operator commands are accurate and secure is a major concern surrounding the remote operation and monitoring of a nuclear reactor. The proposed DTCS framework is designed to address these concerns by using two digital twins of the microreactor to verify and validate sensor data and commands communicated between the remote operations center for trustworthiness and accuracy. In the context of this paper, *verify* refers to an assessment of the authenticity and integrity of data transmitted between the facilities, while *validate* refers to an assessment of the accuracy of the data transmitted, i.e., does the data received represent the true state of microreactor instrumentation and control system.

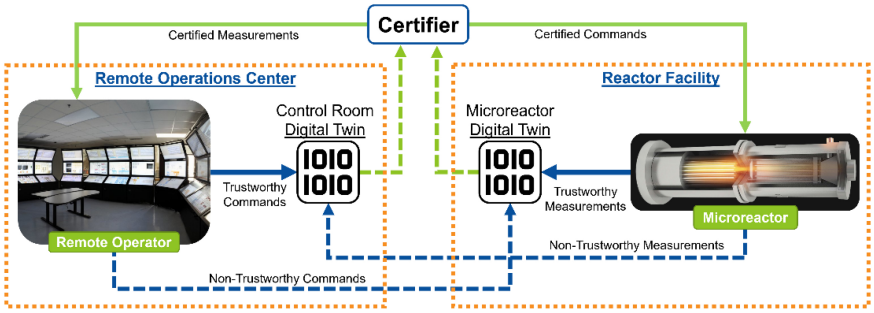

Figure 1: Digital twin certification system general architecture.

The DTCS is constructed in the following manner and the framework can be seen in Figure 1. One digital twin, referred to as the control room digital twin (DT-CR), is located in the remote operations center with a direct, local connection to the operator controls. This digital twin runs simulations predicting future states of the reactor based on trusted operator issued commands and unverified received sensor measurements. The second digital twin,

referred to as microreactor digital twin (DT-MR), is located within the reactor facility physical protection area with a direct, local connection to the supervisory control and data acquisition system. DT-MR uses trusted sensor data and unverified received operator commands as inputs to the simulations. Both digital twins will simulate the microreactor's behavior, and the outputs of the simulations will be used as inputs to the verification and validation process. Agreement between the two digital twins verifies the received information and validates the overall trustworthiness and accuracy of system states predicted by each digital twin.

For resiliency and security, the two digital twins are not identical model implementations. The digital twin in the control room, DT-CR, is a generic, fleet-wide model of a given microreactor production run and is intended to recreate the average behavior of the reactor model in question. As such, this digital twin is based on the microreactor model's nominal design parameters. The digital twin located within the reactor facility, DT-MR, is intended to be representative of the specific microreactor sited within the reactor facility and incorporating its unique operating history. DT-MR is highly tuned to the specific reactor it represents, accounting for the uniqueness of the specific reactor, such as manufacturing tolerances or maintenance differences, relative to the rest of the reactor model fleet. The DT-MR design is based upon the federated-learning framework, a machine-learning technique that trains one global model based on the data of separate, local models (Li et al., 2020). This dual-DT approach leads to several important benefits: (1) the unique implementations of DT-CR and DT-MR provide cyber resilience because if one digital twin is comprised by a bad actor, detailed knowledge of the other digital twin model cannot be gained; (2) any updates to or retraining of DT-CR and DT-MR are based solely on data from trusted, local sources thus eliminating the attack surface of manipulating data transmitted between facilities in an attempt to compromise the DT-CR and DT-MR; and (3) independent digital twins provide an additional diagnostic aid in the case of anomalous system behavior.

COMMAND USE CASE

This section addresses the information exchange that is needed for the DTCS to verify commands before they are implemented at the microreactor. This use case assumes all systems are operating as expected, and communication channels were tested and are secure. It is also assumed that the operator can trust their view of the current state of the microreactor, and integrity is maintained for all transmissions sent.

The human operator is located in the remote operation center, where they monitor reactor operations and make high-level operational decisions. The human-machine interface (HMI) allows the operator to interact with the control/monitoring system. It depicts key sensor values necessary for understanding the current microreactor operating state as well as to allow all necessary commands to be sent. The DT-CR is located in the remote operating center with the operator. The DT-MR is located within the reactor facility with the microreactor. For verifying commands sent from the remote operations center to the reactor facility, the DTCS certifier (C-MR) is used. The

C-MR is a software system that receives and compares the outputs from both digital twins and makes a determination of the authenticity, integrity, and safety of the received command.

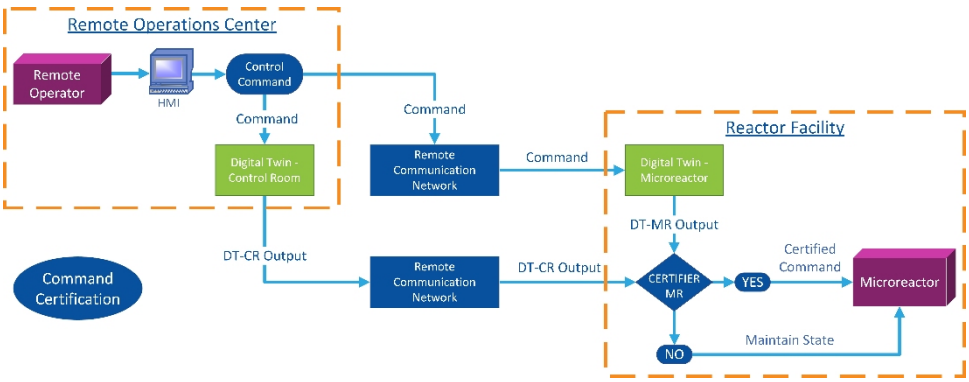

Figure 2: Command certification signal flow and actors.

The method for sending and verifying a command with the DTCS is depicted in Figure 2 and follows the steps below:

1. The remote operator decides what command to implement based on the current operational state of the microreactor. It is assumed that the operator has validated the current state of the microreactor and has the necessary information to make safe and accurate decisions. The operator will input the control action through the HMI.
2. The HMI takes the operator's input and creates a digital control signal that is sent to both DT-CR and DT-MR through independent and secure communication channels.
3. Both the DT-CR and DT-MR compute the future state of the reactor resulting from the command received from the HMI. Then, the outputs of both digital twins are sent to the C-MR for comparison.
4. The C-MR comparison will diagnose whether the control action is authentic, maintains integrity, and is safe. If the control action is verified, the command is sent to the microreactor.
5. A command acknowledgment is sent to both digital twins, confirming that the command was accepted by the microreactor.
6. The control action is finalized, and the microreactor moves forward with implementing the verified command.

This process works to verify the command signal sent to the microreactor, because the DT-CR has a direct, trusted connection to the operator. The command sent to the microreactor facility and DT-MR must be transmitted via the communications network and needs to be verified before it is implemented by the microreactor. Therefore, if the trusted results from the DT-CR match the results of the DT-MR, it can be concluded that the command that reached the reactor facility was the same command provided to DT-CR, thus confirming that the transmitted command is in fact what the operator

sent from the remote facility. Additionally, if the results of the two digital twins do not match, then the system has identified that the received command is not the same as what the operator intended; therefore, the command is not implemented, the operator is alerted, and diagnostic procedures are taken.

MEASUREMENT USE CASE

The previous section described how the DTCS is used for verifying and validating a command sent from the remote operator to the microreactor. The current state of the microreactor would need to be validated before a command can be sent from the operator. This section details how, under normal circumstances, the DTCS is used to verify and validate the sensor data of the operating state from the microreactor. The actors for implementing this process include the microreactor, DT-CR, DT-MR, HMI, and the control room certifier (C-CR).

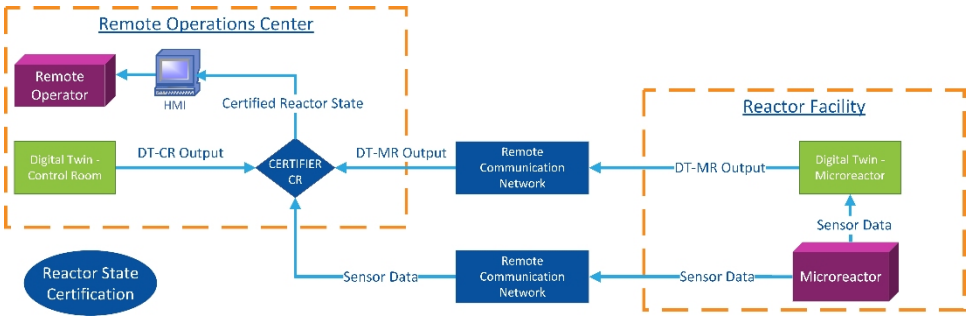

Figure 3: Reactor state certification signal flow and actors.

The process for verifying the state of the microreactor with the DTCS is shown in Figure 3 and follows the sequence below:

1. The sensors on the microreactor capture the data for the current operating state and the data transmitted locally to DT-MR and remotely to DT-CR.
2. DT-CR and DT-MR use a sparse set of the received data to run their simulations and output the expected full reactor state. The outputs from both digital twins are sent to the C-CR.
3. The C-CR compares simulated results and physical sensor data to verify the transmitted data and make a diagnosis on the validity of the data. If the data is confirmed to be trustworthy and accurate, a signal confirming the microreactor state is sent to the HMI, DT-CR, and DT-MR.
4. With the operating state verified, the C-CR will send the microreactor sensor data through to be displayed by the HMI. The HMI will be displaying the last known valid state of the microreactor to the operator at all times.

This method for confirming the microreactor state is effective because the connection between the microreactor sensors and DT-MR is direct and secure since it is a local, wired connection. So, just like with the command verification, one digital twin will provide simulation results using trusted inputs while the other will provide simulation results using not-yet-validated inputs. Therefore, if DT-CR results match the DT-MR, it can be concluded they used the same input indicating the signals sent over the communications network are trustworthy. A second comparison between the expected state of the reactor provided by DT-CR and DT-MR and the microreactor sensor data can then be conducted to assess whether the received microreactor sensor data is an accurate representation of the true state of the reactor.

CERTIFIER FUNCTIONALITY

The purpose of the certifiers, both C-CR and C-MR, is to assess the outputs of each actor in the system, the DT-CR, DT-MR, and the microreactor, and determine whether the outputs of each actor meet a set of verification criteria. Meeting the verification criteria ensures that any information exchanged between facilities, namely commands and reactor state, is authentic, safe, and accurate. If the verification criteria of C-MR are met, the command sent from the remote operations center will be issued to the microreactor. If the verification and validation criteria of C-CR are met, the remote operator can be assured that the reactor state received is an authentic and accurate representation of the true microreactor state. If the outputs of each actor do not meet the verification or validation criteria, C-MR will reject the received command, and C-CR will reject the received state of the microreactor. Rejection from either certifier will alert the operator of an anomaly within the system and the need for the execution of diagnostic procedures.

Verification Criteria: C-MR

The purpose of C-MR is to determine whether commands received by the microreactor are validated and safe via physical verification on top of the cybersecurity measures in place to protect communication channels. The verification process is performed in the following manner, and the signal flow is as shown previously in Figure 2. The output of DT-CR and DT-MR are received by C-MR. The outputs of DT-CR and DT-MR are a prediction of the microreactor's future state. These predictions are in the form of a time series evolution of the microreactor system state or a discrete future state of the microreactor. It is then the responsibility of the certifier to assess the likelihood that these two outputs were the result of the same command. In the likely case that these two outputs were the result of the same command, it can be concluded the command received by the DT-MR is indeed authentic. In this case, the output of DT-CR and DT-MR are evaluated for safety. If this predicted resulting state is determined to be safe and within the performance envelope of the microreactor, the command can be passed along

to the microreactor and executed. In the case it is determined that the outputs of DT-CR and DT-MR are not the result of the same command, the command is not passed to the microreactor, and alerts are sent throughout the system that a command could not be verified. In the case the outputs of DT-CR and DT-MR are likely to be the result of the same command, but this output fails the safety check, the command is not sent to the microreactor, and an alert is sent throughout the system that an unsafe command has been received.

Verification and Validation Criteria: C-CR

The purpose of C-CR is to verify the microreactor state sent from the reactor facility to the remote operations center and to validate the received state, assessing if the received state is an accurate representation of the true state of the microreactor. The signal flow of this process is as shown previously in Figure 3. This verification and validation check is performed in the following manner. The outputs of DT-CR and DT-MR, which are provided to C-CR, are a prediction of the microreactor's complete current state made based upon a sparse set of sensor data received directly from the microreactor in the case of DT-MR and communicated from the microreactor to the remote operations facility in the case of DT-CR. In addition to the digital twin outputs, the full set of received reactor-state data as well as the historical state of each digital twin and the reactor are provided to the C-CR. It is then the responsibility of the C-CR to assess the likelihood that these two outputs were the result of the same input data set, i.e., the data set received by DT-CR is the same data set directly provided to DT-MR by the microreactor, and the digital twin outputs and received reactor state are congruent with the historical states (i.e., dynamics are reasonable). If the state estimates from both digital twins are not congruent with their respective historical states, then diagnostics are run. If they are congruent with historical states, then five possible outcomes are a result of this assessment and are given in Table 1. Case 1 represents the agreement between all actors and results in the approval of the reactor's state, which means the state received at the remote operations center is likely the true state of the reactor. Cases 2–5 represent the disagreements between some or all actors and the diagnostic procedures needed to confirm the true state of the reactor. These diagnostic procedures aim to determine the root cause of the discrepancy whether it be a physical problem, such as a failed or malfunctioning sensor or reactor component, or a digital problem, such as a malfunctioning digital twin or a cyberattack on an actor in the system.

Table 1. State validation possible outcomes.

Case	Scenario	Action
Case 1	$DT_{CR} = DT_{MR} = MR_{State}$	Approve
Case 2	$DT_{CR} \neq DT_{MR} = MR_{State}$	Diagnose Fault
Case 3	$DT_{MR} \neq DT_{CR} = MR_{State}$	Diagnose Fault
Case 4	$DT_{CR} = DT_{MR} \neq MR_{State}$	Diagnose Fault
Case 5	$DT_{CR} \neq DT_{MR} \neq MR_{State}$	Diagnose Fault

FUTURE DEVELOPMENT AND TESTING PLANS

This paper has described the DTCS functionality under normal operating conditions when all systems, including communication networks, reactor sensors, etc., are operating as designed. However, the DTCS is intended to add operational resilience specifically in abnormal operation scenarios. In addition to confirming operation under ideal conditions, there are adverse scenarios (briefly described in Table 2) that are planned for further testing of the system. These test scenarios were chosen because they are possible concerns when dealing with a remote operations system. The purpose of the DTCS is to increase signal trustworthiness from operational and security perspectives, and the goal of this testing is to show the system can handle these abnormal or threat scenarios and potentially identify areas for improving the system's resiliency.

It is expected that the DTCS will be able to identify when a measurement transmitted from the reactor to the remote control center is due to a degraded or failed sensor and not actually a physical abnormality within the reactor. If a sensor has degraded, and bad data is sent to the remote operations center, the digital twins will be running their simulations with data from the previously verified state when the sensor was still intact for comparison within the C-CR. The contrast of normal digital twin results to sensor data that does not match would indicate that the sensor(s) may be degrading.

Table 2. Additional testing scenarios.

Test Type	Possible Scenario
Abnormal physical conditions	A degraded/failed sensor input
Cyber-threat conditions	Man-in-the-middle attack
Unauthorized user	An unauthenticated command is sent

A man-in-the-middle attack is a cyber threat where the attacker alters the communications being sent between two parties. An example of this for the remote operation of a microreactor would be the attacker altering the command signal that is sent from the remote operator to the DT-MR. That signal is transmitted over the communications network to the microreactor facility. Well implemented secure communication channels should preserve the confidentiality, integrity, and authenticity of a message. However, if proper encryption and security methods are not used, the message could be intercepted and modified by an attacker. The DT-CR is in the remote operations facility with the operator and receives the command signal via a direct connection. It is not a transmitted signal intercepted by an outside attacker. So, the DT-CR will run its simulation with the intended command. The DT-CR results will be sent separately from the command action signal transmission. Gaining access to one signal would not grant access to the other, and gaining access to both and injecting logical messages would raise the difficulty for an adversary. Therefore, the C-MR would detect a difference in DT-MR and DT-CR and the command would not go through to the microreactor.

The scenario of an unauthorized user would occur when anyone other than the approved operators gains access to an authorized access point within the system and sends a command. This is a complicated threat scenario for the DTCS to handle. While the DTCS does not prevent an unauthorized user from sending a command, it will prevent dangerous commands from being sent to the microreactor. Every command sent is simulated by both digital twins before it is implemented by the microreactor. If a dangerous command is sent by an unauthorized user, the simulation results from the digital twins will indicate that the command will cause problems within the system, and it will not be implemented. The utilization of digital twins will allow the DTCS to show that it is an unsafe command and prevent its execution, but this scenario does warrant further consideration of whether it is possible to bypass this check in the system.

The purpose of doing these tests is to confirm that the DTCS addresses problems as expected but also to identify potential problems that would require further testing/research. This is a novel concept and system framework, so it will require a significant amount of testing to confirm its efficacy in providing suitable security and resiliency to remote operations.

CONCLUSION

Remote operation and monitoring are crucial for the successful implementation of microreactors. Other industries have utilized remote operation and monitoring, and the concept can be applied to nuclear applications. The proposed digital twin remote operations framework was created with the goal of providing the level of security, resilience, and safety required for nuclear power systems.

This paper introduced the concept of a DTCS framework to be utilized in the remote operation of microreactors. The novel implementation of digital twins introduced in this framework raises the security and resiliency of remote operation and monitoring to the level required by the nuclear industry. The two individual digital twins work as an additional tool for identifying the cause of any system anomalies in addition to providing extra layer of security to the transmitted information. Future work will further define specific implementation solutions for the DTCS concept. The DTCS will be used to support remote operation of a test facility, with specific test scenarios to evaluate the command and state verification and validation capabilities.

ACKNOWLEDGMENT

The authors would like to acknowledge the support of Troy Unruh, Haydn Bryan, 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

Araújo, K., Black, G., Shropshire, D., & van Heek, A. (2022). Prospects for nuclear microreactors: A review of the technology, economics, and regulatory considerations. *Nuclear Technology, 209*, 1–20.

Fan, Y., Li, L., Lin, K., & Tse, M. (2020). A review of applications in federated learning. *Computers & Industrial Engineering, 149*, 1-15.

Fang, S., Dong, H., Liu, M., & Xu, C. (2021). Review of digital twin about concepts, technologies, and industrial applications. *Journal of Manufacturing Systems, 58*, 346–361.

Grieves, M. (2014). Manufacturing excellence through virtual factory replication. *White Paper*, 1–7.

Hepsø, V., & Monteiro, E. (2021). From integrated operations to remote operations: Socio-technical challenge for the oil and gas business. In *Proceedings of the 21st Congress of the International Ergonomics Association (IEA), 219*, 169–176.

U. S. Department of Energy. (2022). *National cyber-informed engineering strategy.* Final Report, 1–37.