Human Error, Reliability, Resilience, and Performance, Vol. 82, 2023, 33–42
https://doi.org/10.54941/ahfe1003551

Digital Twin Verification for Advanced Reactor Remote Operations

Thomas A. Ulrich, Joseph Oncken, Ronald L. Boring, Kaeley Stevens, Megan Culler, Stephen Bukowski, Troy Unruh, and Jeren Browning

Idaho National Laboratory, Idaho Falls, ID 83415, USA

ABSTRACT

Advanced reactors, especially microreactors, must take advantage of remote monitoring and control strategies to reduce the commercial cost of deployment and operations costs to compete with existing electrical generators. A robust and flexible remote concept of operations must be developed to support diverse designs and use cases to ensure safe and reliable operations. This paper presents the unique aspects of remote operations as they contrast existing established operations to highlight issues that must be considered. A key element of the remote operations concept is the ability for a physically separated command and control center to maintain awareness of the reactor's state and perform supervisory control on the reactor. A digital twin implementation is proposed to serve as a verification system, to provide the remote operations center with verified reactor state information and to provide the remotely situated reactor with verified operation center commands. This approach augments existing communication infrastructure to support operators as they assess the validity of the information they are receiving and confidence that the commands they issue can be executed at the remote reactor.

Keywords: Remote operations, Concept of operations, Advanced reactor, Fission battery, Digital twin

INTRODUCTION

The nuclear industry is pursuing advanced reactor designs to meet growing and increasingly diverse electric demands of the modern U.S. grid system. Many of these advanced reactor designs are nearing sufficient maturity to begin to consider test deployments. Working with Idaho National Laboratory, for example, the prototype reactors will initially be tested and overseen by human operators onsite to monitor the systems until confidence in the hardware design and the control system is obtained. Commercial deployment considerations will swiftly follow as designers begin to develop concepts of operations. Given there are many different designs, the concept of operations may vary proportionally; however, there are a few key concepts within envisioned operations that will likely be common across most of the prevailing designs. Remote operation is an operating philosophy that will more than likely be incorporated into a large portion of advanced reactors' concepts of operations.

This paper first presents the concept of remote operations with an emphasis on contrasting against traditional onsite operations. Benefits over traditional onsite operations and the challenges that must be addressed to achieve remote operations provide the context to optimize a potential implementation. The second half of the paper then presents a possible implementation based on digital twins, providing a means for operators to verify data signals between the remote operations center and the reactor facility. This paper presents a preliminary study design aimed to address these unique remote aspects of operations with an evaluation of a preliminary concept of operations and an accompanying human-machine interface (HMI) developed to validate the digital twin operator support capability.

CONCEPT OF REMOTE OPERATIONS

Ontology of Remote Operations

The commercial nuclear power industry has yet to fully develop or deploy a remote concept of operations for a nuclear reactor. As such, the concept itself is still somewhat ill-defined. The term itself is not new, and numerous industries including oil and gas, military and civilian aerospace, regional electric grids, etc. have developed remote concepts of operations. Nuclear can draw upon the greater maturity in surrogate industries to inform the development of a nuclear remote concept of operations. The essential definition obtained from these other domains is found in a U.S. Nuclear Regulatory Commission (NRC) report that characterizes remote operations as a configuration in which "the command and control location is far removed from the feature that is controlled" (NRC, 2022). Though not explicitly stated within this definition, there are several basic assumptions associated with the physical separation between the remote operations center and the reactor. There are over a dozen reactor vendors with unique designs, and therefore some assumptions do not apply equally to each design. However, vendors pursuing remote operations should consider these assumptions as they pertain to any remote concept of operations in which a reactor is being monitored and controlled from a remote location. Before presenting the assumptions, it is first worth delineating the type of advanced reactors that are favorable for remote operations.

Key Advanced Reactor Characteristics

All advanced reactor designs have two basic requirements. First the design of the reactor is intended to reduce the initial capital investment to eliminate many of existing barriers that have prevented the U.S. from continuing to build large scale, gigawatt capacity reactors. Advanced reactor vendors are targeting two capacity size categories, which are small modular reactors and microreactors. Small modular reactors and microreactors are defined with capacity definitions of less than 300 MW and 2–50 MW, respectively. The smaller capacities and the modular design reduce the cost significantly. The reduced capacity can support smaller consumers or groups of consumers that either do not need or could not afford the immense initial capital investment required for a full 1-gigawatt traditional reactor. Furthermore, the reduction in scale simplifies the planning, siting, and construction, since the reactors are sufficiently small that they can be manufactured by the vendor and shipped intact to their siting location, as opposed to traditional reactors, which must largely be built onsite around key components that are shipped piecemeal. In some cases, small modular reactors may be pooled together to create a larger overall electrical output. For example, the NuScale Power reactor design features up to 12 modules (i.e., individual reactors) linked together to produce nearly a gigawatt of electricity; yet the cost of building 12 modules is lower than the cost of building a single reactor of similar power output. Collectively, advances in technology to fabricate these reactors and the reduced scale provide greater flexibility in their deployment and have provided a much simpler adoption strategy that has significantly less risk.

In addition to the capacity scale, the second fundamental design requirement for advanced reactors is inexpensive operating costs. This objective is achieved by relying on passive safety systems that eliminate much of the need for active human operators to continuously monitor these reactors to ensure their safety. To ensure longevity and reduce component failure rates, designs focus on eliminating moving parts in favor of passive systems that rely on the natural physics such as convection to circulate coolant and transfer heat. These designs aim to reduce operating costs below existing and competing forms of electrical generation by using the metric of $/kW hour. The second basic requirement for advanced reactor designs is the operational costs with respect to other forms of electrical generation in terms of $1/kW hour.

The work described in this paper is part of a larger project supporting the development of fission battery technologies, deployment strategies, and operations. Fission batteries are a specific variant of microreactors defined by the five following characteristics (Forsberg, Foss, & Abou-Jauode, 2022):

1. Economic – Must be cost competitive with other distributed electric generators
2. Standardized – Scale and capacities standardized to support factor production similar to production rates for commercial airplanes
3. Installed – Modular and transportable such that a unit can be shipped to a central facility for maintenance instead of onsite
4. Unattended – Operated securely and safely in an unattended manner without operators onsite
5. Reliable – Robust systems to support the unit throughout mission life

Many of these characteristics are also present in other scale advanced reactor designs. Fission batteries are unique in their unattended operations and installed modularity, which is also sometimes referred to as plug-and-play. As such, fission batteries can be quickly installed without significant siting accommodation and then run semi-autonomously until they are removed from service for replacement or refurbishment. Fission batteries, which represent an extreme end of the autonomy spectrum, are still only semi-autonomous as opposed to autonomous, since they do require some level of remote monitoring and control to adjust electrical power output based on grid demands.

They also require the ability to monitor and remove the unit from service at the end of life or for servicing. Removal from service is the primary issue that requires human oversight, and therefore even with automatic generation control, fission batteries require some level of human intervention. To enable human operators to monitor and perform limited control of fission batteries, a remote operation scheme is necessary and central to transmit and receive sensor information and controller commands.

Long Distance Communication

The distal relationship requires communication between the operations center and the remote reactor. Traditional power plants achieve this communication through analog instrumentation and control systems with miles of cabling linking the equipment in the plant to the control room where operations are conducted. Existing commercial reactors maintain security barriers around the plant, which provides an extensive level of defense against natural hazards and malicious actors from damaging the communication line systems sufficiently to cause an interruption of communication between the field equipment and the control room. In contrast, an advanced reactor deployed with a remote concept of operations is inherently unable to establish a protected barrier around the operations center and the remote reactor. Instead, the remote operations must use existing network infrastructure or construct their own dedicated network infrastructure to support communication. Developing, constructing, and maintaining an entire communication infrastructure to support remote operations is economically prohibitive. Therefore, remote operations will likely be forced to rely on existing infrastructure that is not under the direct control of the utility operating the reactor. The net result is one of the fundamental assumptions that remote operations must be capable of maintaining oversight of the remote reactor while using potentially untrusted communication networks with no guarantee of uninterrupted communications. The operators manning the operations center must be able to appropriately calibrate trust in the incoming information signals from the remote reactor to respond appropriately. Therefore, from a human factors perspective, the HMIs must be capable of presenting the incoming information with cues to the information reliability as well as providing guidance on cross-validating information sources to arrive at some confidence as to the true state when information is disparate due to interrupted or corrupted communications. Given the assumed lapses in communication, a level of autonomy is also assumed as part of the future remote concept of operations.

Autonomous Instrumentation and Control

The level of autonomy depends on the design of the specific advanced reactor, but in general advanced reactors are aiming towards higher levels of autonomy in which the reactor could function without oversight, as is the case for fission battery designs. Industry can and will achieve this, but the first wave of deployments, even if they had the autonomous capability, would not operate independently of humans until the technology gathers a track record of high reliability. Therefore, remote reactors will have some functionality built into the control system that is self-reliant and constraint based. For example, safety functions, such as the reactor protection system, require no command to SCRAM the reactor to shut down criticality. This is not new technology, as traditional reactors also have automated reactor protection systems that actuate independently. However, operational functions, such as power adjustments that might require increasing reactivity, would be initiated by an operator. Therefore, a human operator will in the foreseeable interim have constant oversight and actively monitor and occasionally transmit control commands to the reactor.

Operator Role

The existing fleet of commercial reactors exhibit very little autonomy and automation. Operators build their mental model of the plant state by positioning themselves in front of a particular system panel, finding the appropriate indicator, and reading and interpreting the value. The operators rely on procedures to guide them through combinations of indicators to determine the plant state. Operators are also extensively trained to recognize and diagnose key sets of plant states that require swift resolution. After diagnosis, operators follow logic within the procedures for appropriate actions to return the plant to safe state. The logic also guides operators through routine plant evolutions to ensure the proper sequencing of interim configurations towards an overall end state, i.e., maneuvering the plant from a cold shutdown to online and full power after a refueling outage.

Operators have access to some digital systems in existing control rooms. For example, the safety parameter display system, which is a post three-mile island requirement (Woods et al., 1981) displays key plant parameters to support operators in quickly obtaining plant states during emergency situations. Plant control is still largely manual, with tedious individual component control manipulations. There are some digital systems that provide basic automation to configure systems of controls collectively. Numerous plants have adopted digital turbine control systems, which allow operators to perform supervisory control at the system level, such as setting a turbine ramp rate setpoint. The control system then manipulates turbine inlet steam valves to move the turbine to the setpoint speed. Despite some advancement, existing operations require a high number of manual actions at a fine resolution control in stark contrast to the envisioned operations for advanced reactors, especially remote operations.

The fine level control of individual system elements is not desirable or feasible for remote operations due to several factors. First, the reliability of the communication cannot be ensured. Additionally, fine resolution control requires short-time duration feedback cycles that could exceed communication time lags and cause challenges to operators attempting to fine tune a particular process. As such, the remote reactor control system will perform most if not all fine resolution control actions after receiving a supervisory control command at the system level from the operator. A system level control command refers to a sequence of individual control actuations to achieve the desired system state. Other industries such as aviation have adopted similar supervisory control, known as fly-by-wire. The pilot is not directly altering the airframe's surface actuators, but instead control inputs from the cockpit are sent to a controlling computer that determines the individual control actions required to achieve the intended effect. For example, the pilot may move the yoke to the right. This command is sent to the aircraft's control system to determine the appropriate surface actuator adjustments to create the aerodynamics required to bank the aircraft to the right. Much the same as some advanced reactors, some airframes require complicated, minute, and short time duration control to maintain stability that are beyond human capabilities.

The control system also provides safeguards since it can identify pilot actions that may be unsafe and could compromise flight stability. The pilot must be clearly informed as to why the action could not or should not have been executed. A failure to address this issue can lead to pilots losing situation awareness and is one factor in the recent string of Boeing 737-Max crashes in which the automation overrode pilots' commands to pull the nose the aircraft up due to a faulty sensor (John & Harris, 2019). Pilots were unable to adjust or override the automation, and several planes crashed as a result resulting hundreds of deaths.

Remote operations can draw upon the advancements in the aviation industry, as well as others such as teleoperation in robotics (Bruemmer et al., 2005), by adopting the same supervisory control approach. The operator never performs fine resolution control and instead commands the remote reactor to change an overall system state. Advanced reactors, especially those using remote operations, will not provide remote controls for manipulating the equipment with specific component level manipulations in lieu of higher-level supervisory control commands.

The limited high-level functional control approach is advantageous for operations for several reasons. First, since the communication cannot be guaranteed at any given timepoint, the operator cannot execute specific control actions for activities that are time sensitive and require immediate follow-up actions. The physical process is underway and proceeds regardless of whether the operator has lost communication with the reactor. Therefore, sending the supervisory system level control command is a favored approach for executing remote commands. Additionally, the supervisory control approach limits operator actions and can more reliability be communicated without ambiguity. The control system can validate the operator-issued command with clear beginning and end system level states implicitly conveyed by the encapsulation. Individual control actions can be much more difficult to evaluate since there is no inherent goal state associated with most individual control actions. Collectively, the autonomous functionality provides a more constrained set of actions for the operator remotely overseeing the reactor than what is currently performed by operators in traditional existing nuclear power plants. The limited suite of control capabilities afforded to the remote operator raises another assumption concerning expertise. As noted by the Nuclear Regulatory Commission, remote operations may not require operators trained and certified to the rigorous and extensive levels of existing operators

(2022). This assumption is less clear than the others due the potential for centralizing oversight of fleets of remote reactors to operations centers.

Aggregated and Centralized Operations

Operations aggregation and centralization are intertwined concepts associated with the distally located command and control scheme. Most if not all remote operation designs aim to aggregate oversight of geographically disparate reactors to a central operations center or series of centers. There are use cases for remote operations focusing on a single reactor connected to challenging or hazardous location with a microgrid configuration (Shropshire, Black, & Araujo, 2021). Indeed, the main economic drivers are remote locations in which the other electric power sources, such as diesel generators, are costly to operate due to fuel transportation costs and logistical demands. To be economically viable, a convergence between remote reactors and fewer operations centers is likely required and yields increasing economy of scale as the ratio of remote reactors to operations centers increases. For example, a ratio of 100:1 of remote reactors to operations centers is much more cost effective than a ratio of 5:1. The aggregation of oversight for multiple remote reactors to a single operations center has significant implications for human factors considerations for future remote concept of operations.

Remote System State Verification

Given that the communication infrastructure is fallible, as it is outside the system boundary due to the physical separation between the operations center and the remote reactor, operators must have the ability to confidently acquire the state of the remote reactor. A robust and well-designed communication infrastructure and protocol is necessary to harden against cybersecurity or naturally occurring communication disruptions. However, these measures are not sufficient to entirely prevent cybersecurity vulnerabilities or eliminate communication failures. Instead, a more pragmatic approach entails assuming the communication will be disrupted or partially corrupted, within reason, and then design a mechanism to compensate for a limited and tolerable level of communication issues. One method to contend with communication issues is to implement a verification process that can provide the remotely situated operators with a high degree of confidence as to which aspects of the communicated system states are accurate reflections of the actual reactor state. The system sends redundant outcomes to the operators so that operators are aware of communication breakdowns and reduce the uncertainty of the true plant state based on the available signals they are receiving even if some are missing or corrupted. One approach to the verification issue is actively being pursued by an internally funded Idaho National Laboratory project using reactor digital twins to support the verification.

Digital Twin Decision Support Tools

The term digital twin has become a buzzword across many domains and as a result it is important to explicitly convey what the term means within the

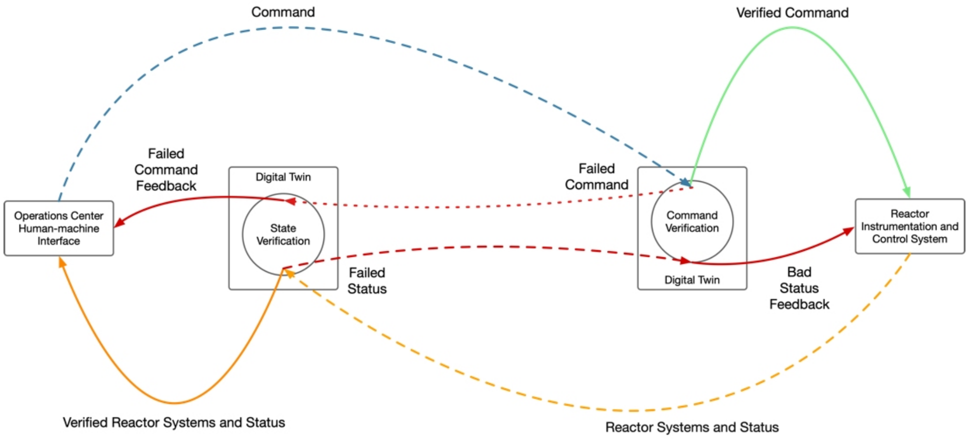

Figure 1: Proposed digital twin communication verification method.

nuclear context. Jones et al. (2020), provide an excellent overview of 12 characteristics associated with digital twins based on an extensive literature review. Three of the characteristics are inherent to any digital twin and serve as the basic definition for the concept. To be considered a digital twin there must be a physical entity, a digital replica of that entity, and some data connection to support data exchange between the physical entity and digital replica. Beyond this, digital twins can have additional characteristics specific to their application as is the case for digital twins proposed for the verification application to support remote operations.

The graphic below depicts a verification implementation with two digital twins, one at the remote operations center and the other at the remote reactor site. The operations center digital twin verifies incoming reactor status against historic and predicted future reactor state models. The remote reactor digital twin verifies incoming commands against the reactor instrumentation and control system as well as predicted future states to ensure the execution of the received commands is safe and appropriate. The digital twin models that the larger research team is actively developing to support the project are based on physical testbeds and have the capability to predict process parameters, but the ability to control the process to the required accuracy has yet to be realized (Ritter, Hays, & Browning, 2022). Furthermore, as this is still an early phase of the project, the dual digital twin approach must be developed for the microreactor application and systems. As the digital twin modelling continues to advance, the method for updating the models to account for operational changes to the system and synchronize the models while ensuring their integrity must be developed.

CONCLUSION

This paper presented an overview of the unique characteristics of advanced reactors that shape the concept of remote operations vendors and utilities must develop prior to any reactor being deployed. Additionally, this paper aimed to further formulate the definition of remote operations issued by the

Nuclear Regulatory Commission in the Future Focused Research Initiative Report (2022). Fortunately, the design of advanced reactors establishes an inherent high level of safety and autonomy; however, there are still many challenges distally distinct reactors pose to their operations. These challenges must be addressed by future research, and this paper provides one potential approach to improve the overall performance of remote concept of operations by providing digital twins as a form of communication verification to ensure the remote command center is aware of the true reactor state and the commands sent to the reactor are appropriate and unmodified. The next phase of this research will focus on developing and executing an evaluation study focusing on the concept of operations with the simplified simulator, Rancor (Ulrich, 2017; Park et al., 2023), representing the advanced reactor; a wizard of oz, emulated digital twins implementation; and scenarios developed to evaluate breakdowns in command and control. The study aims to understand how an operator can make use of the digital twin to maintain their situation awareness of the reactor state and perform appropriate supervisory control. The study is still in the planning phase, but key issues include explainable and transparent artificial intelligence to allow the operator understand issues and by the digital twins and attribute the issue to the appropriate source, i.e., cyber-attack, communication loss, sensor or controller failure, or physical component failure. Others are encouraged to pursue similar studies to investigate other challenges facing the nuclear industry as they move closer to deploying the first generation of remote reactors.

ACKNOWLEDGMENT

This work of authorship was prepared as an account of work sponsored by Idaho National Laboratory, an agency of the United States Government. Neither the United States 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. Idaho National Laboratory is a multi-program laboratory operated by Battelle Energy Alliance LLC, for the United States Department of Energy under Contract DE-AC07-05ID14517.

REFERENCES

Bruemmer, D. J., Few, D. A., Boring, R. L., Marble, J. L., Walton, M., & Nielsen, C. (2005). Shared understanding for collaborative control. *IEEE Journal of Systems, Man, and Cybernetics--Part A: Systems and Humans, 35,* 494–504.

Forsberg, C., Foss, A., & Abou-Jaoude, A. (2022). Fission battery economics-by-design. *Progress in Nuclear Energy*, *152*, 104366.

Johnston, P., & Harris, R. (2019). The Boeing 737 MAX saga: Lessons for software organizations. *Software Quality Professional*, *21*(3), 4–12.

Jones, D., Snider, C., Nassehi, A., Yon, J., & Hicks, B. (2020). Characterising the Digital Twin: A systematic literature review. *CIRP Journal of Manufacturing Science and Technology*, *29*, 36–52.

Nuclear Regulatory Commission (2022). *Ground Rules for Regulatory Feasibility of Remote Operations of Nuclear Power Plants* (Future Focused Research Initiative Report).

Park, J., Yang, T., Boring, R. L., Ulrich, T. A., & Kim, J. (2023). Analysis of human performance differences between students and operators when using the Rancor Microworld simulator. *Annals of Nuclear Energy*, *180*, 109502.

Ritter, C., Hays, R., Browning, J., Stewart, R., Bays, S., Reyes, G.,... & Zohner, P. (2022). Digital twin to detect nuclear proliferation: A case study. *Journal of Energy Resources Technology*, *144*(10), 102108.

Shropshire, D. E., Black, G., & Araújo, K. (2021). *Global Market Analysis of Microreactors* (No. INL/EXT-21-63214-Rev000). Idaho National Laboratory (INL), Idaho Falls, ID (United States).

Ulrich, T. A., Lew, R., Werner, S., & Boring, R. L. (2017, September). Rancor: a gamified microworld nuclear power plant simulation for engineering psychology research and process control applications. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting, 61,* 398–402.

Woods, D. D., Wise, J. A., & Hanes, L. F. (1981, October). An evaluation of nuclear power plant safety parameter display systems. *Proceedings of the Human Factors Society Annual Meeting, 25,* 110–114.