INL/CON-23-71255-Revision-0

DEMONSTRATION OF A MULTI-STAGE TESTING AND EVALUATION APPROACH FOR A SAFETY-RELATED DIGITAL UPGRADE AT A NUCLEAR POWER PLANT

Casey R Kovesdi, Paul Joseph Hunton, Jeremy David Mohon

Changing the World's Energy Future

Idaho National Laboratory

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

INL/CON-23-71255-Revision-0

DEMONSTRATION OF A MULTI-STAGE TESTING AND EVALUATION APPROACH FOR A SAFETY-RELATED DIGITAL UPGRADE AT A NUCLEAR POWER PLANT

Casey R Kovesdi, Paul Joseph Hunton, Jeremy David Mohon

October 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

APPLICATION OF A MULTI-STAGE TESTING AND EVALUATION APPROACH FOR A SAFETY-RELATED DIGITAL UPGRADE AT A NUCLEAR POWER PLANT

Casey R. Kovesdi, Paul Hunton, and Jeremy Mohon
Idaho National Laboratory

There is an imminent need for existing United States nuclear power plants to reduce their operating and maintenance costs to remain economically viable. Digital technology provides significant opportunity for the existing nuclear power plant fleet to transform that way in which work is accomplished to reduce costs and allow the fleet to remain economically competitive. However, a careful understanding of the human-technology integration is needed to ensure the continued safe and reliable operation of these existing plants with new digital capabilities. This work presents interim findings in applying human factors engineering to a safety-significant digital upgrade for a United States nuclear power plant, following the new Alternative Review Process in the recently revised Digital Instrumentation and Control Interim Staff Guidance Licensing Process, Revision 2. The interim results described in this work provides an industry perspective, based on ongoing work, to support recent work published from Vazquez, Green, and Desaulniers (2022).

INTRODUCTION

Nuclear power provides approximately 20% of electricity generation to the United States (U.S.). Nearly half of the nation's non-greenhouse-gas-emitting electric power generation is nuclear power, providing a significant role in mitigating climate change. However, existing nuclear power plants are being challenged economically as other electricity generating sources, like natural gas and renewable energy sources, have seen reduced operating and maintenance (O&M) costs for a variety of reasons, including changes to the energy market, as well as added government subsidies for resources like solar and wind (Remer, Thomas, Lawrie, Martin, & O'Brien, 2021). As a result, there is an imminent need for existing nuclear power plants to reduce their O&M costs to remain economically viable.

Digital technology, including automation, provides significant opportunity for the existing nuclear power plant fleet to transform that way in which work is accomplished to reduce O&M costs and allow the fleet to remain economically competitive. Research by Remer and colleagues (2021) identified several nuclear power plant work domains and associated opportunities to develop, demonstrate, and deploy innovative solutions that include digital technologies to significantly reduce O&M costs to enable continued operation of the existing U.S. nuclear power plant fleet. For instance, Remer and colleagues (2021) investigated critical work domains that provide the greatest opportunity for O&M cost savings in the next 3–5 years.

The challenge is that existing instrumentation and control (I&C) technologies in the main control room (MCR) are highly analog, costly to operate and maintain, and demand high levels of cognitive and physical workload from plant staff (i.e., operators). Digitalizing the MCR has a range of broad economic benefits, including:

- Improved testing and surveillance with digital technology in a way that improves existing processes
- Reduced need for skill-of-the-craft in the maintenance (i.e., diagnosing, troubleshooting, and maintenance) of I&C systems
- Improved plant operations resulting from improved handling of technical specifications, communication between MCR and field, and overall crew situation awareness
- Overall obsolescence management.

Digital I&C systems can fundamentally change the way in which plant staff operate the plant; this is known as the concept of operation. Operators who once adapted to and leveraged the characteristics of the analog I&C in existing MCRs will be impacted using digital technologies. Some examples of notable changes may include:

- Transitioning from standing to seated workstations
- Using large overview displays for sensemaking as opposed to relying on the vast amounts of readily viewable analog indications
- Using data visualization techniques and integration to support situation assessment, diagnosis, and response planning
- Managing alarms differently as a result of new capabilities that filter and prioritize incoming alarms
- Using computer-based procedures that offer new capabilities unseen in paper-based analogs
- Using increased levels of automation to control the plant, which changes operation from tactical (i.e., at-the-boards) to more supervisory.

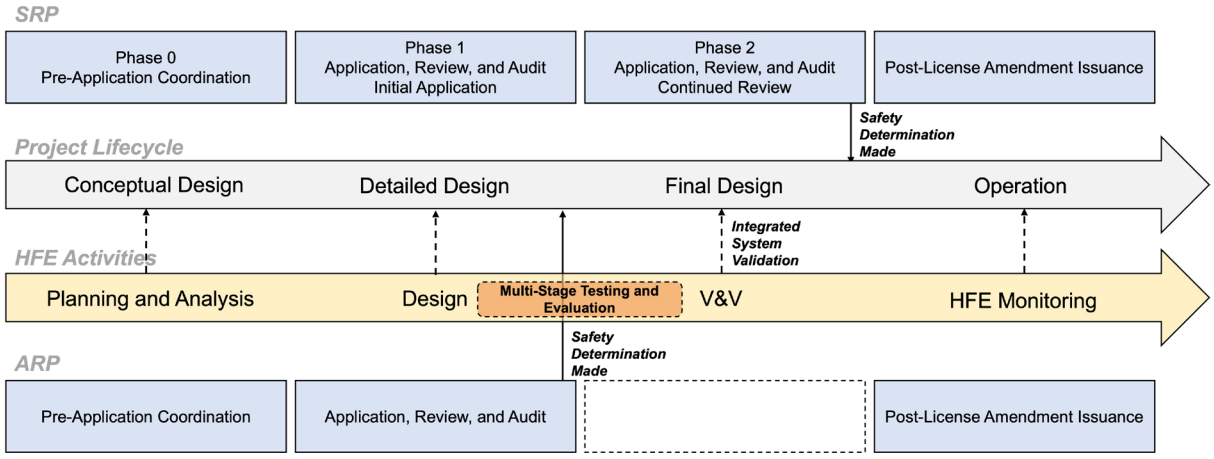

Figure 1. Generalized process differences between SRP and ARP in DI&C-ISG-06.

These characteristics indeed require careful understanding of the human-technology integration considerations that are part of changing the concept of operation. For instance, assigning plant functions to people and automation (i.e., function allocation) requires understanding the capabilities of both people and the technology (i.e., automation) at hand. Human-technology integration employs human factors engineering (HFE) methods and principles to maximize the benefits of digital technology while reducing human error traps.

This work presents interim findings in applying HFE to a safety-significant digital I&C upgrade for a U.S. nuclear power plant, following the new Alternative Review Process (ARP) in the recently revised *Digital Instrumentation and Control Interim Staff Guidance* (DI&C-ISG-06) *Licensing Process*, Revision 2, (2018). The specific results coming from this work have been omitted. This work provides an industry perspective to recent work published from Vazquez, Green, and Desaulniers (2022).

In this paper, an overview of the ARP-DI&C-ISG-06 process is given and challenges it brings in applying HFE as part of the licensing submittal is discussed. This work presents preliminary findings in following a multi-stage testing and evaluation (MS-T&E) approach that has been applied to this work in effort to overcome the challenges. The intent of this work is to support industry in following a MS-T&E approach that may be used for addressing HFE in safety-significant digital I&C upgrades at U.S. nuclear power plants.

CHARACTERISTICS OF THE ARP-DI&C-ISG-06

Recently revised DI&C-ISG-06 (2018) provides two processes for a licensee (utility) and regulatory review of a digital I&C LAR. These including the Standard Review Process (SRP) and the recently developed ARP. The intent of the ARP is to enhance clarity and streamline the process by reducing the amount of docketed material and increased the focus of information needed to reach a safety determination. The enabler for the ARP in providing this efficiency is from the omission of the Phase 2 review. This is depicted in Figure 1, above.

When following the Alternate Review Process, the license amendment request (LAR) is submitted to the NRC and can be approved by the NRC prior to factory acceptance testing (FAT), as opposed obtaining LAR approval after FAT in the Standard Review Process. This is visualized in Figure 2 by the safety determination being made much earlier when following the ARP, as opposed to the SRP.

The value of using the ARP is to shorten the schedule for obtaining LAR approval (reducing project schedule risk) and obtain NRC technical approval before FAT (reducing technical and associated cost risks) associated with receiving and resolving NRC requests for additional information at the end of the design and test cycle. The key prerequisite in allowing an applicant to pursue the ARP is to leverage a safety platform that has already received a generic safety evaluation report (SER).

THE ROLE OF HFE IN DI&C-ISG-06

HFE is referenced in DI&C-ISG-06 as an element to be addressed. The licensee is expected to describe the framework used to design and develop the digital I&C safety-related systems and this includes performing "*appropriate human factors engineering for the human-system interfaces throughout the development process*" (DI&C-ISG-06, Section D.4.1 [p. 41]). Specific standards that apply to HFE in DI&C-ISG-06 can be traced to Institute for Electrical and Electronics Engineers (IEEE) 603 (2018) and IEEE 1023 (2020).

The HFE guidance in IEEE 1023, as referenced in DI&C-ISG-06, uses a general engineering process model described as the Star Model, which allows for diversity of acceptance processes in actual situations in performing digital modifications (2020). This guidance centers around recommended practices for applying HFE to systems and equipment that include safety-significant human-system interfaces (HSIs; i.e., referred to as 'significant human interfaces') across the system lifecycle. The role of HFE is also a critical element in DI&C-ISG-06 by nature of being part of the regulatory review guidance: NUREG-0800 Chapter 18 (2016). NUREG-0800 Chapter 18, Human Factors

Engineering, references NUREG-0711 (2012) and NUREG-1764 (2007) as primary technical resources.

NUREG-0711 provides guidance for the regulator to review the licensee's submittals of modifications and new builds; however, the guidance is often considered "good engineering practice" and is followed by applicants as a general HFE process, when also accounting for a graded approach (EPRI 3002004310, 2015). The guidance between NUREG-0711 and IEEE 1023 are in essence complementary to each other; although, the Star Model presented in IEEE 1023 is more general and not intended to be applied at face value (IEEE 1023, 2020).

HFE CHALLENGES IN FOLLOWING THE ARP

Referring to Figure 1, the safety determination can be made earlier in the project life cycle when following the ARP. However, also seen in Figure 2, HFE integrated system validation is completed much later in the process. As discussed in Vazquez and colleagues (2022), the absence of integrated system validation test results limits the regulatory review of validation activities in accordance with NUREG-0711. This creates a unique challenge such as by (A) either requiring the licensee to expedite the schedule in completing necessary HFE activities leading into validation or (B) requiring the regulator to make a safety determination in the absence of integrated system validation results.

Vazquez and colleagues (2022) is one of the first to present possible solutions in addressing this challenge. Leveraging IEEE Std 2411 (2021), the authors offer a multi-staged approach as a basis for validating the proposed digital I&C modifications. Here, early-stage results within the multi-staged validation program using a limited-scope simulator could alleviate scheduling constraints regarding the use of a full-scope simulator such as used in integrated system validation. This multi-staged approach is discussed in detail in Vazquez and colleagues (2022).

Here, integrated system validation is not eliminated, but is incorporated within the broader validation approach. Here, the regulator may be able to make a safety determination prior to the integrated system validation test results. These earlier tests would need to sufficiently demonstrate that the proposed design maintains reasonable assurance of plant safety. The validation guidance in NUREG-0711 should be considered as deemed applicable for earlier validation activities. For instance, considerations such as sampling of operational conditions, selection of performance measures and validation criteria, and test procedures should be considered as appropriate to earlier-staged testing to which a safety determination may be made.

The next section discusses how this safety-significant digital I&C project, following the ARP, is working to following a MS-T&E approach.

DEMONSTRATION OF A MS-T&E APPROACH

Human factors engineers and I&C engineers at the Idaho National Laboratory are leading the HFE efforts for a safety-significant digital I&C project at a major U.S. utility, following the first-of-a-kind ARP process. This work is following guidance from INL/EXT-21-64320 (2021). Figure 2 outlines the generalized phases described in this report.

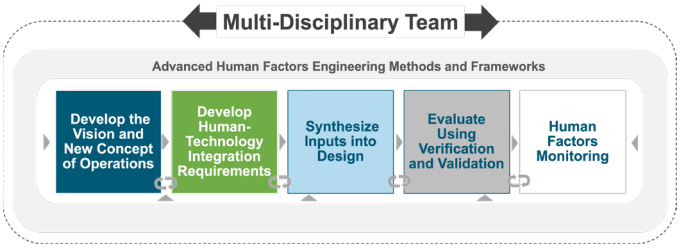

Figure 2. Human and technology integration methodology.

The methodology shown in Figure 2 addresses key HFE activities described in both NUREG-0711 and IEEE 1023. It also translates to the industry-accepted systems engineering framework, termed the Digital Engineering Guide (DEG), developed by the Electrical Power Research Institute (EPRI). The DEG is also being used in this project to manage the broader set of engineering activities across the lifespan of the project (Hunton et al., 2022).

The HFE Program Plan for this project, developed in guidance with INL/EXT-21-64320, leverages guidance from NUREG-0711 in addressing elements as appropriate, following a graded approach in executing HFE technical activities (e.g., task analysis). To date, the project has performed technical HFE activities that cover the broader Planning and Analysis umbrella and is currently performing activities related to Design (Figure 3).

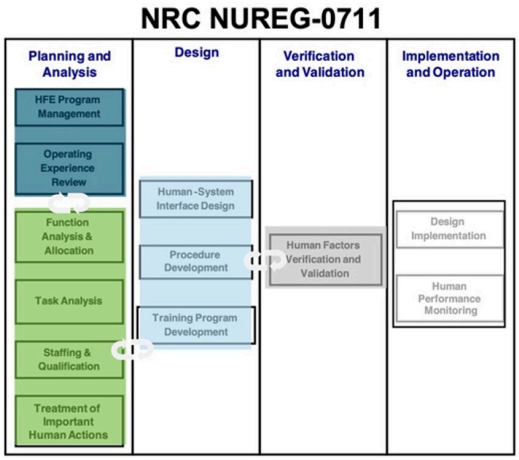

Figure 3. NUREG-0711 with INL/EXT-21-64320 phases overlaid.

The HFE efforts have also adapted other necessary inputs from relevant standards and guidelines to address the challenge posed by following the ARP, which is to enable a safety determination before integrated system validation. The standards and guidelines used include IEEE 2411 (2021), NUREG-0800 Chapter 18 Attachment A (2016), and NUREG-1852 (2007) to establish a MS-T&E approach. A driver for this approach was to minimize the scheduling burden in addressing necessary HFE considerations while following the ARP.

A notable adaption to the NUREG-0711 model (Figure 3) was that the project included two additional tests and evaluations as part of the MS-T&E strategy in the transition from design into verification and validation:

- ***Conceptual Verification (Added)***
- ***Preliminary Validation (Added)***
- Design Finalization
  - *Includes HFE Design Verification and Task Support Verification activities.*
- Integrated System Validation
  - *Includes Planning, Execution, and Human Engineering Discrepancy Resolution.*

These two activities were developed by leveraging the guidance in NUREG-0800 Chapter 18 Attachment A (Guidance for Evaluating Credited Manual Operator Actions), Phases 1 and 2, respectively. The purpose of these activities were to support the design of the new HSIs, and serves in part of a broader MS-T&E effort to build reasonable confidence that the new HSIs and modified procedures can be effectively used by the plant personnel to safely and reliably operator the plant. Referring to Figure 1, these four activities are illustrated by the orange overlay between Design and V&V on the set of HFE activities. It is also emphasized that integrated system validation, as described in NUREG-0711 (2012), is part of the MS-T&E approach described here. The next sub-sections summarize the characteristics of conceptual verification and preliminary validation.

Conceptual Verification

The goal of conceptual verification is to verify that the HSIs being developed along with associated modification to the procedures are progressing towards an acceptable state to enable preliminary validation. This is determined by following the HFE Program Plan, by following the results from earlier Planning and Analysis activities, and by leveraging the guidance in NUREG-0800 Chapter 18 Attachment A Phase 1.

Conceptual verification is accomplished using independent teams with distinct roles to minimize bias. These teams include the design team, simulator team, validation team, and HFE process team. During this activity the results from Planning and Analysis activities (e.g., function analysis and allocation and task analysis) are used as inputs into the sampling of operational conditions, identification of important tasks, and the design of the new HSIs and procedure changes.

The design team's role is to develop conceptual HSIs and modify procedures to support the use of these HSIs, following important tasks identified from the site's risk analyses and incorporated into scenarios. These scenarios comprise a set of impacted tasks identified during the Planning and Analysis activities; the tasks are incorporated into scenarios by the simulator team and were selected based on their degree of difficulty, importance, and frequency.

The HFE process team performs expert reviews on the conceptual HSIs using the HSI style guide and following guidance from NUREG-0700 (2002). Findings from this review are provided back to the design team for disposition in preparation for conceptual verification. This activity uses walkthrough analysis in a part-task glasstop simulator, following the developed scenarios.

The fidelity and scope of the simulator configuration is part-task in nature, and limited functionality to focus on the navigation between HSI display pages and overall content of each display. That is, the MCR layout is presented using a limited-scope simulator (e.g., glasstop simulator with four bays) where the HSIs are primarily static in nature, with only navigation between display pages active.

The scenarios demonstrate impacted safety-important tasks as identified by the utility, and from their risk analyses, to provide early assurance that the HSIs and procedures can be effectively used in performing these impacted tasks.

Another important element of conceptual verification is to establish acceptance criteria for the impacted safety-important tasks. Leveraging guidance from NUREG-0800 Chapter 18 Attachment A Phase 1 (2016), the time available to perform these actions is established by the utility and per deterministic and probabilistic risk analysis documentation. Estimated times to perform these actions are derived by facilitating the walkthrough analysis with the validation team (i.e., these are qualified operators). The sequence of actions necessary for the operators to operate the plant in these tasks using available alarms, indications, and controls are recorded and documented using operational sequence diagrams (OSDs). The OSDs are then used to create timelines following the guidance in NUREG-1852 (2007) to conceptually verify that the operators can effectively use the new HSIs and modified procedures within the time available for these tasks.

Conceptual verification also evaluates the impacts of the new HSIs and procedures across a broad range of impacted tasks that are captured in the scenarios. Conceptual verification therefore enables evaluating the new HSIs and modified procedures in other plant tasks and evolutions of high importance to access the acceptability and overall usability of these interfaces.

An outcome of conceptual verification is the development of a set of acceptance criteria to enable preliminary validation. The criteria is based on regulatory requirements and benchmarks of existing human-system performance to provide additional assurance. Conceptual verification also provides a level of assurance that the operators can safely and reliably operator the plant using the alarms, controls, displays, and other equipment that remain functions, as captured in the scenarios.

Preliminary Validation

Building on the results of conceptual verification, a primary goal of preliminary validation is to provide high confidence that the impacted safety-important tasks will be accomplished correctly, reliably, and within the time available, using the new HSIs and modified procedures. Preliminary validation is a performance-based tests that utilizes the same scenarios and tasks captured in conceptual verification. However, preliminary validation is demonstrated in a test environment that is of higher fidelity, including a fully configurable glasstop simulator (e.g., see Figure 4).

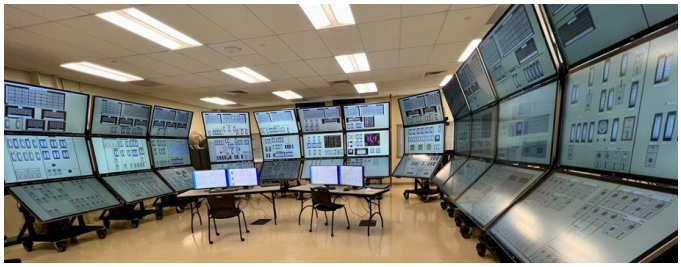

Figure 4. Photograph of the Human System Simulation Laboratory.

The testbed also uses the site simulator model and the new HSIs include increased functionality. Specifically, the HSIs needed to perform the safety-important actions are functional, interacting with the plant model data, allowing for navigation, and enabling the use of soft controls to operate impacted plant equipment. Timing data can be collected in greater fidelity. It should be noted that the testbed is still limited scope, as compared to what is typically used in integrated system validation. Here, tasks performed with the existing analog controls and indications are simulated by the simulator team; this is done since the simulator is configured on glasstop bays and the physical interaction with these controls are not physically represented. Additionally, certain changes in automation are simulated by the simulator team to enable early evaluation of human-system performance for new plant these evolutions.

The HFE process team collects an array of qualitative and quantitative measures to address considerations including impacts to human-system performance, workload, situation awareness, and overall system usability. Human factors engineers collect observations and unsolicited comments through audio/video recordings and available software tools. Timing data is captured to construct the timelines, following guidance in NUREG-1852 (2007). Finally, workload and situation awareness is evaluated using industry-accepted survey instruments. Ultimately, the purpose of preliminary validation is to provide early-stage results within the MS-T&E framework that can be used to support the regulator with making a safety determination in support of LAR approval. As previously noted, preliminary validation is not meant to replace or omit integrated system validation. Rather, it served as one milestone within a broader MS-T&E framework.

CONCLUSIONS

This work presents interim results of performing HFE to support significant digital modifications to a U.S. nuclear power plant while following the ARP in DI&C-ISG-06 (2018). The benefit of the ARP offers a streamlined process in obtaining a LAR approval, which reduces scheduling and project risk. This reduced timeframe, however, has created a unique challenge with addressing HFE for these upgrades, as current regulatory guidance, NUREG-0711, focuses on the reliance of integrated system validation to make a safety determination. Recently, Vazquez and colleagues (2022) have proposed possible approaches in allowing the regulator to make a safety determination before integrated system validation by following a multi-staged validation approach. This work demonstrates the planning and execution of a MS-T&E that leverages such guidance, among other industry standards and guidelines including NUREG-0711 (2012), NUREG-0800 Chapter 18 Attachment A (2016), and IEEE 2411 (2021). The interim results described in this work here may be one such path in allowing HFE to be integrated into the ARP. As the project continues, additional lessons learned will be developed and shared with industry.

ACKNOWLEDGMENTS

This manuscript has been authored by Battelle Energy Alliance, LLC under Contract No. DE-AC07-05ID14517 with the U.S. Department of Energy. The United States Government retains and the publisher, by accepting the article for publication, acknowledges that the U.S. Government retains a nonexclusive, paid-up, irrevocable, world-wide license to publish or reproduce the published form of this manuscript, or allow others to do so, for U.S. Government purposes.

REFERENCES

Digital Instrumentation and Controls Interim Staff Guidance #06, Revision 2, Licensing Process. Washington, DC: U.S. Nuclear Regulatory Commission.

Hunton, P, England, E., Herrell, D., Lawrie, S. & Samselski, M. (2022). Safety-Related Instrumentation and Control Pilot Upgrade: Initial Scoping Phase Implementation and Lessons Learned. *Nuclear Technology, 209*(3), 366-376.

IEEE. 2021. "Guide for Human Factors Engineering for the Validation of System Designs and Integrated Systems Operations at Nuclear Facilities." IEEE 2411. Institute of Electrical and Electronics Engineers.

IEEE. 2020. "Recommended Practice for the Application of Human Factors Engineering to Systems, Equipment, and Facilities of Nuclear Power Generating Stations and Other Nuclear Facilities." IEEE 1023. Institute of Electrical and Electronics Engineers.

IEEE. 2018. "Standard Criteria for Safety Systems for Nuclear Power Generating Stations." IEEE 603, Institute of Electrical and Electronics Engineers.

Kovesdi, C., Z. Spielman, R. Hill, J. Mohon, T. Miyake, and C. Pedersen. 2021. "Development of an Assessment Methodology That Enables the Nuclear Industry to Evaluate Adoption of Advanced Automation." INL/EXT 21 64320, Idaho National Laboratory.

Remer, J., K. Thomas, S. Lawrie, K. Martin, and C. O'Brien. 2021. "Process for Significant Nuclear Work Function Innovation Based on Integrated Operations Concepts" INL/EXT 21 64134, Idaho National Laboratory.

U.S. Nuclear Regulatory Commission. 2007. *Demonstrating the Feasibility and Reliability of Operator Manual Actions in Response to Fire,* NUREG 1852, U.S. Nuclear Regulatory Commission.

U.S. Nuclear Regulatory Commission. 2007. *Guidance for the Review of Changes to Human Actions*, NUREG-1764. Rev 1, U.S. Nuclear Regulatory Commission.

U.S. Nuclear Regulatory Commission. (2012). *Human Factors Engineering Program Review Model*, NUREG-0711, Rev. 3. Washington, DC: U.S. Nuclear Regulatory Commission.

U.S. Nuclear Regulatory Commission. (2002). *Human-System Interface Design Guidelines*, NUREG-0700, Rev. 2. Washington, DC: U.S. Nuclear Regulatory Commission.

U.S. Nuclear Regulatory Commission. 2016. *Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants - Human Factors Engineering*, NUREG-0800, Chapter 18, Rev. 3, U.S. Nuclear Regulatory Commission.

Vazquez, J. A., Green, B. D., & Desaulniers, D. R. (2022). Regulatory Considerations for the Potential Use of a Multi-Stage Validation Testing Approach to Support Human Factors Engineering Technical Reviews for Proposed Nuclear Power Plant Control Room Design Modifications. *Proceedings in the Human Factors and Ergonomics Society Annual Meeting, 66*(1), 1381–1385.