SANDIA REPORT
SAND2020-5635
Printed June 2020

Sandia National Laboratories

Human Factors Considerations for Automating Microreactors

Elizabeth S. Fleming, Megan Nyre-Yu, and David L. Luxat

Prepared by
Sandia National Laboratories
Albuquerque, New Mexico
87185 and Livermore,
California 94550

Issued by Sandia National Laboratories, operated for the United States Department of Energy by National Technology & Engineering Solutions of Sandia, LLC.

Available to DOE and DOE contractors from
U.S. Department of Energy
Office of Scientific and Technical Information
P.O. Box 62
Oak Ridge, TN 37831

Telephone: (865) 576-8401
Facsimile: (865) 576-5728
E-Mail: reports@osti.gov
Online ordering: http://www.osti.gov/scitech

Available to the public from
U.S. Department of Commerce
National Technical Information Service
5301 Shawnee Rd
Alexandria, VA 22312

Telephone: (800) 553-6847
Facsimile: (703) 605-6900
E-Mail: orders@ntis.gov
Online order: https://classic.ntis.gov/help/order-methods/

ABSTRACT

The U.S. Nuclear Regulatory Commission (NRC) has interacted with vendors pursuing the commercialization of microreactors (< 10 MW_{th}). It is envisioned that microreactors could be assembled and fueled in a factory and shipped to a site. Many of the sites are expected to be remote locations requiring off-grid power or in some cases military bases. However, before this new class of nuclear reactor can be fully developed and implemented by designers, an effort must be made to explore the technical issues and provide reasonable assurance to the public regarding health and safety impacts centered on various technical issues. Prior works have examined many of these issues.

One issue not yet fully explored is the possible change in role of the operations and support personnel. Due to the passive safety features of microreactors and their low level of nuclear material, the microreactor facilities may automate more functions and rely on inherent safety features more than its predecessor nuclear power plants. In some instances, human operators may not be located onsite and may instead be operating or monitoring the facility from a remote location. Some designs also call for operators to supervise and control multiple microreactors from the control room.

This report explores the issues around reduced staffing of microreactors, highlights the historical safety functions associated with human operators, assesses current licensing requirements for appropriateness to varying levels of personnel support, and describes a recommended regulatory approach for reviewing the impact of reduced staff to the operation of microreactors. The report evaluates these issues through an extensive literature survey and Subject Matter Expert interviews. The literature covers research topics related to Human Factors Engineering as well as regulatory guidance given by the Nuclear Regulatory Commission.

ACKNOWLEDGEMENTS

This work is overseen and funded by the U.S. Nuclear Regulatory Commission as part of the Non-Light Water Reactor Policy and Technical Guidance Support, Risk-Informed, Performance-Based, Technology-Inclusive Regulatory Infrastructure.

Thank you to Dr. Paul Schutte for his peer review.

CONTENTS

LIST OF FIGURES

LIST OF TABLES

This page left blank

ACRONYMS AND DEFINITIONS

Abbreviation	Definition
BWXT	Babcock & Wilcox Technologies
CFR	Code of Federal Regulations
ConOps	Concept of Operations
DOT	Department of Transportation
EPRI	Electric Power Research Institute
FAA	Federal Aviation Administration
HABA-MABA	Humans Are Better At – Machines Are Better At
HFE	Human Factors Engineering
HI-SMUR SMR-160	Holtec Inherently-Safe Modular Underground Reactor
HMI	Human-Machine Interface
HRA	Human Reliability Analysis
IED	Intelligent Electronic Devices
IAEA	International Atomic Energy Agency
INCOSE	International Council on Systems Engineering
INSAG	International Nuclear Safety Group
IP	Implementation Plan
ISV	Integrated System Validation
LANL	Los Alamos National Laboratory
LoA	Level of Automation
LWR	Light Water Reactor
NASA	National Aeronautics and Space Administration
NEI	Nuclear Energy Institute
NPM	NuScale Power Module
NPP	Nuclear Power Plant
NRC	Nuclear Regulatory Commission
NREL	National Renewable Energy Laboratory
OER	Operating Experience Review
PRA	Probabilistic Risk Assessment
RO	Reactor Operators
SA	Situation Awareness
SCADA	Supervisory Control and Data Acquisition
SME	Subject Matter Expert
SMR	Small Modular Reactor

Abbreviation	Definition
SRK	Skills, rules, and knowledge-based behaviors
SRP	Standard Review Plan
SSC	Safety systems, structures, or components
STPA	System-Theoretic Process Analysis
UAV	Unmanned Aerial Vehicle
UUV	Unmanned Underwater Vehicles
W-SMR	Westinghouse Small Modular Reactor

1. INTRODUCTION

1.1. Background

Over the past several years, there has been a significant stakeholder interest in the development and licensing of non-light water reactors (LWRs). Through this interest, questions surrounding policy and key technical issues associated with licensing and deploying advanced reactor designs need to be answered. A subset of advanced reactor designs needing particular attention is microreactors, which are typically smaller (in physical size, radioactive material inventory, etc.), more reliant on passive or inherent design features, and most likely to propose significant departures from existing regulatory requirements and guidance. Specifically, many of these designs seek to use minimal, if any, onsite human staff. Site operations may include partially or fully autonomous systems.

A passive safety system is one for which there is no reliance on external inputs to achieve the desired safety function. In a passive safety system, the safety function is achieved through reliance on laws of nature, material properties, and energy stored within the safety systems, structures, or components (SSC). Passive safety within microreactor design is intended to ensure that the reactor will fail-safe and be self-regulating. Additionally, the reactors are expected to be less complex with less active components. With a passive safety system, a microreactor design would not require significant human or automation intervention to maintain a safe state. Thus, human and/or automated tasks may serve as a secondary safety check rather than a primary function to operate the reactor.

While many of these sites may incorporate autonomous systems, there is no clear definition regarding how automation will be used at the various microreactor sites. Further, there's even less understanding of how humans will be involved in on-site and remote decision-making and tasks. The design of an autonomous, or partially autonomous, system must be approached with careful consideration of the goals of the system. The system goals must be defined through careful input by a variety of stakeholders, including, but not limited to, users, managers, affected members of the public, and designers. Once the goals are understood, the functions for how those goals are achieved can be decomposed and allocated to components within the system. Those functions are then connected with human-driven tasks for how to complete the function. At this stage, a designer must consider how much they want the human to control in the system versus how much they want the machine to control. How will the human engage with the system? At the lowest automation level, the human makes all the decisions with no help from the automation. From there, the machine may offer recommendations or different decision-paths to help the human with their task. At the highest level, the machine, including inherent physical characteristics and supporting analog or digital control systems, decides and executes everything, with no input or supervision from the human.

A key aspect in the design of microreactors is specifying the level of automation within the system and how much the human will be engaging with that system. For the various levels of automation, there are critical issues that arise that must be explored within the literature. This report is the initiation of a discussion into the factors that influence automation within microreactors.

This document:

- explores the issues around reduced staffing of microreactors;
- highlights historical safety functions associated with human operators;

- assesses current licensing requirements for appropriateness to varying levels of personnel support; and
- describes a recommended regulatory approach for reviewing the impact of reduced staffing to the operation of microreactors.

1.2. Scope

This report provides key insights from research and current regulation to guide the discussion around automating microreactors. This work does not provide requirements for staffing numbers, define specific human tasks, or design training. Additionally, the presented work does not establish new policy definitions or regulation guidance. Instead, guidance from both the human factors domain and NRC regulations are integrated to establish a common language, key definitions, and to integrate findings from past research.

The report is organized as follows:

- Section 2 explores the issues around reduced staffing of microreactors through a literature review of human factors engineering (HFE) topics.
- Section 3 highlights the historical safety functions associated with human operators in a nuclear power plant (NPP) and assesses the current licensing requirements for NPPs using a combination of literature and NRC guidance.
- Section 4 overviews the findings of Subject Matter Expert interviews and highlights literature on current microreactor designs to show how both HFE literature and NRC guidance might integrate with the new reactor designs.
- Section 5 addresses gaps to applying current methods to microreactor designs by outlining a proposed recommended regulatory approach for reviewing the impact of reduced staffing to the operation of microreactors.

2. HUMAN-SYSTEM INTEGRATION AND AUTONOMY

Human Factors Engineering (HFE) "uses knowledge of human abilities and limitations to design systems, organizations, jobs, machines, tools, and consumer products for safe, efficient, and comfortable human use." (Human Factors and Ergonomics Society, n.d.) HFE considers how humans interact with a system and how system design might impact those interactions. To adequately integrate HFE considerations, human factors perspectives and analyses must be included early in the design process and continuously integrated into the design throughout the whole process (INCOSE Systems Engineering Handbook, 2015). Therefore, human factors literature was reviewed for guidance on important areas of concern when automating microreactors.

The purpose of this literature review is to help provide some guidance for assessing risks between human operators and microreactors. As the design specifications for the new technology is neither widely available nor common across providers, this literature review will present some foundational concepts around determining

1. what inputs are needed for a human to safely operate complex technology;
2. what level of automation is appropriate to support each human interaction with the technology, and;
3. terms, models, and methods that can be applied in this context.

Finally, this literature review will provide examples from other industries that have similar applications of human supervisory control in complex system to create some foundation of how human-automation interaction has been implemented.

2.1. Relevant Theories & Concepts

2.1.1. Human Supervisory Control and Level of Automation

The foundational literature in human-automation interaction discusses concepts of human supervisory control and level of automation (Sheridan, 1992, 2000, 2012, 2016; Sheridan & Ferrell, 1974). Human supervisory control refers to the relationship between humans and autonomous machines, particularly in systems in which the human plays the role of a controller or supervisor. This can range from monitoring, intermittent programming, and active controlling. Human supervisory control is a vital consideration in the design and operation of complex technology (Sheridan & Ferrell, 1974). Therefore, the system requirements are influenced through the designer's understanding of what tasks the human will perform in steady-state operations.
In the same vein, it is important to consider the level of autonomy of the machine (Parasuraman, Sheridan, & Wickens, 2000). Figure 1 below helps describe these levels of automation with respect to human information processing. The paper from which this figure was taken also describes a four-stage model for how to breakdown human interaction based on stages of processing:

1. **Information Acquisition:** Positioning and orienting of sensory receptors, sensory processing, initial pre-processing of data prior to full perception
2. **Information Analysis:** Cognitive operations (rehearsal, integration, inference) before decision making
3. **Decision & Action Selection**
4. **Action Implementation**

The authors also note that these four stages need not have the same level of automation. For instance, automation may assist in information retrieval at a high level, collected needed sensory information to be presented to the operator, with lower levels of automation at the analysis, decision, and action stages. A more automated system might have high level of automation for data collection and analysis, with moderate levels at decision making. This might look like narrowing down the decision space based on known information and completed analysis.

TABLE I
LEVELS OF AUTOMATION OF DECISION AND ACTION SELECTION

HIGH	10. The computer decides everything, acts autonomously, ignoring the human.
	9. informs the human only if it, the computer, decides to
	8. informs the human only if asked, or
	7. executes automatically, then necessarily informs the human, and
	6. allows the human a restricted time to veto before automatic execution, or
	5. executes that suggestion if the human approves, or
	4. suggests one alternative
	3. narrows the selection down to a few, or
	2. The computer offers a complete set of decision/action alternatives, or
LOW	1. The computer offers no assistance: human must take all decisions and actions.

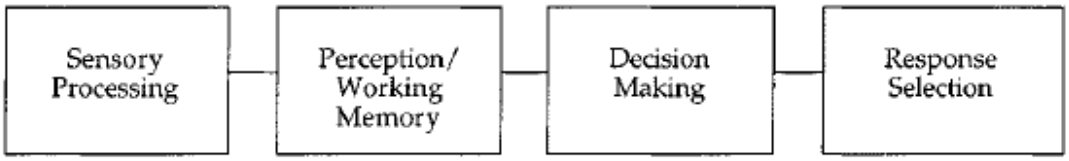

Figure 1. Levels of Automation of Decision and Action Selection (Parasuraman et al., 2000)

Parasuraman et al (2000) also propose a process by which system designers can determine the appropriate level of automation for each stage, with an example of level of automation determination in future air traffic control systems. This process can also be described as ***function allocation***, or determining the distribution of responsibility over tasks between human operators and systems (de Winter & Dodou, 2014; Joe, O'Hara, Hugo, & Oxstrand, 2015; Price, 1985). Function allocation need not be static. Other sub-topics in function allocation literature discuss the need for dynamic function allocation and adaptive function allocation. There is much literature available on function allocation alone. However, the models presented in (Parasuraman et al, 2000) provide a comprehensive approach to function allocation based in human supervisory control and human information processing.

2.1.2. Situation Awareness & Trust

Situation awareness (SA) is another theoretical model commonly discussed with human supervisory control and function allocation (Endsley, 1996). Situation awareness is "a perception of elements in the environment within a volume of time and space, the comprehension of their meaning, and the projection of their status in the near future" (Endsley, 1995, 2000). Essentially, situation awareness is what allows a human operator to gain and maintain cognizance of the system and environment with which they are interacting. Having strong SA allows the human operator to answer questions about what the system is doing, and why it is doing it.

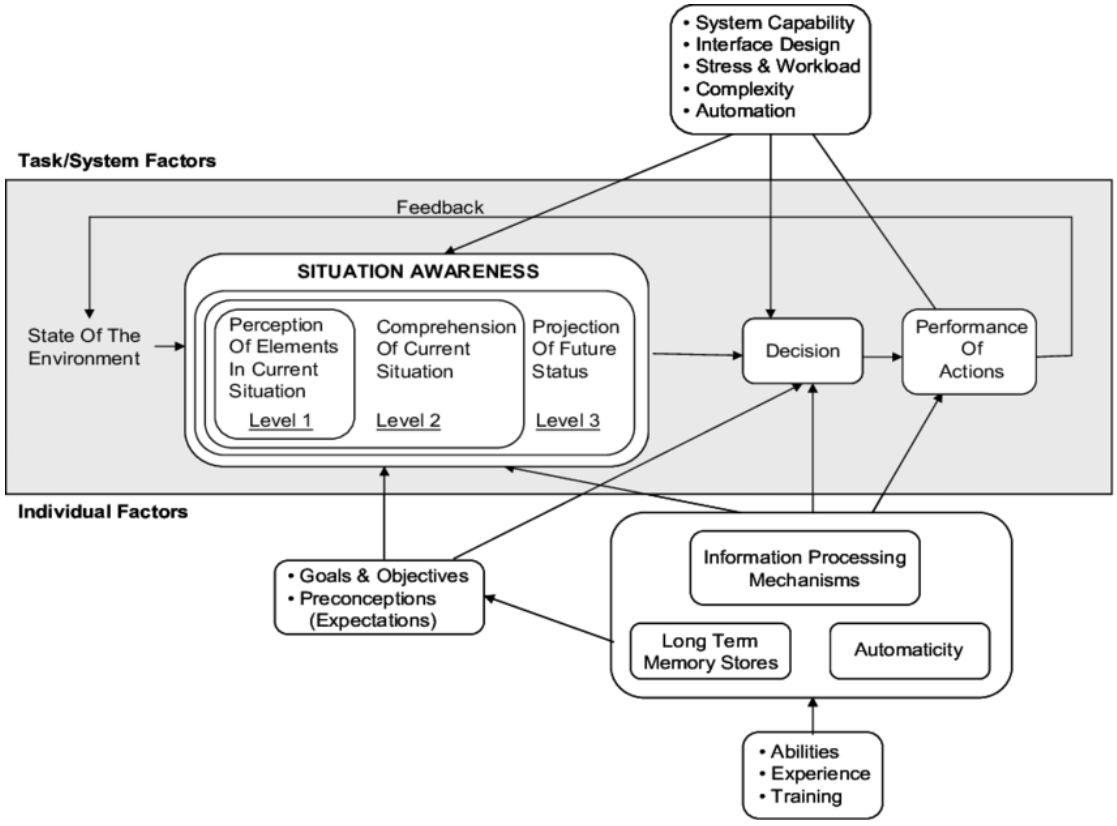

Figure 2. Situation Awareness Model (Endsley, 1995b)

Designing for situation awareness includes understanding needs of the human operator in order to maintain cognizance of the autonomous system. This involves sensors, signals, information presentation, information salience and alerting, analysis of incoming data, decision option presentation, and potentially expected outcomes of decisions. Discussed within the SA research corpus is also the *automation conundrum*, "in which the more autonomy is added to a system, and its reliability and robustness increase, the lower the situation awareness of the human operators and the less likely that they will be able to take over manual control when needed" (Endsley, 2016). Overlapping with this conundrum, Bainbridge (1983) summarized the so-called ***"ironies of automation"***, which highlight many considerations for automation design and deployment. ***Trust*** is also a central component to implementing autonomous systems, especially when a human operator may need to assume control of the technology.

Technology reliability compared to human reliability has been used to justify the development and deployment of autonomous systems. Consequently, the consistent and predictable operation (and appropriate communication) of that technology is expected in order for the human to monitor, react, and control accordingly, as needed. Operators can become overconfident in (and even dependent upon) automation, leading to complacency and a loss in SA (Parasuraman, Sheridan, & Wickens, 2008). These are important considerations for risk assessment of future systems that might involve higher levels of automation.

2.2. Human-Autonomy Systems within Industry

2.2.1. Supervisory Control and Data Acquisition (SCADA) Systems

More applicable examples related to microreactor systems are Supervisory Control and Data Acquisition (SCADA) systems, which encompass wind and solar farms, among others. SCADA systems are often described as distributed sensors or machines that are centrally and remotely monitored and controlled by a human operator (Krambeck, 2015). The physical system components can be directly interacted with by human technicians, but are often designed to be mostly autonomous with advanced technological controls to adjust to different conditions (Ahmed & Soo, 2008; Sayed & Gabbar, 2017). Nevertheless, the importance of well-designed human-machine interface (HMI) has been recognized and studied (Zolotová & Landryová, 2005) to address concerns about time sensitive decision-making in potentially high risk environments.

2.2.1.1. Electric Power Grids

A comparable example of a SCADA system in energy is electric power grid operations. This includes creation, transmission, and distribution processes. Within this domain, research has identified that expertise is needed by human operators to successfully manage control room operations in electric grids (Adams & Hannigan). The literature base has much representation of SA, supporting the need to maintain and even increase situation awareness as grid operations incorporate more automation (Adams et al., 2015; Connors, Endsley, & Jones, 2007; Greitzer, Schur, Paget, & Guttromson, 2008). More specifically, (Giri, Parashar, Trehern, & Madani, 2012) provide examples of different views of grid operations to enhance situation awareness of human operator. They also propose an analytics and visualization framework based on levels of SA and risk management process. (Panteli & Kirschen, 2015) provides a framework for achieving adequate SA in power systems. This includes an iterative process that involves assessment and continuous determination of SA requirements. Outside of human factors literature, there is also work to support computational approaches to SA enhancement in power grids with decision support systems (Naderpour, Lu, & Zhang, 2014).

One key difference between electric power grid research and microreactor development is the current existence of a process to study. In many of the papers provided above, the studies started with current grid operations to understand expertise and SA needs of operators. This presents two caveats for the literature. The first is that, since a microreactor system has not been deployed, this report's assessment of assumed microreactor capabilities may not be accurate. The second caveat follows from the first in that much of the discussed literature may not be appropriate for microreactors, depending on how the reactors are designed and integrated. The Methodological section will propose alternatives for determining appropriate levels of automation, expected task scenarios, and potential needs to support SA and decision making in those contexts.

2.2.1.2. Wind Farms, Solar Farms, and other SCADA Systems

Research-based examples of the design of the HMI for solar and wind specifically are limited. Sayed & Gabbar (2017) provide an overview of wind farms as a SCADA system, with some level of addressing the HMI and the security of the control system. Within solar applications, the need for well-developed SCADA networks and human-machine interface has been recognized in business and pop literature, stating that operators are expected to monitor and quickly act on system alarms to mitigate potential problems (Wood, 2019). The development of HMI for SCADA systems has some literature base in other applications, such as subsea monitoring (Cai et al., 2012) and desalination (Morsi, Deeb, & Zwawi, 2009).

With respect to wind turbine and solar controls, some SCADA systems have been developed and deployed internationally. These systems have some level of automation, but also allow for human interaction and control. Specific aspects of human-machine interaction are not included in the relevant literature, presumably because these systems were developed by private companies making this type of information potentially proprietary.

The Symphony® Plus system is an automation-based distributed control system that helps balance complex, distributed controls and link autonomous energy systems (Timbus & Bitto, 2015). With respect to the human operator, Symphony® Plus advertises that it provides the operator the ability to operate effectively, specifically regarding availability, reliability, redundancy, remote monitoring, communication. This is done through a common system environment that distributes and provides role-based context to control room operators, maintenance engineers, plant optimization engineers, plant managers. Specifically, the literature advertises that Symphony® Plus can "transform to contextual data".

The report about Symphony® Plus indicates that communication between autonomous systems is essential, historically lacking, problematic, and costly. However, there exist some standards for centralized, consolidated operations, which integrate industry standard communication protocols such as IEC 61850, IEC 60870-5/101/103/104, OPC and Modbus TCP. Symphony® Plus also incorporates consolidated alarms and events notifications to help support abnormal situation awareness and effectiveness of operators. Some specific aspects of system design philosophy and integration are included in available reports. Symphony® Plus SD Series controllers are used to integrate intelligent field devices, including transmitters, actuators, motor control centers and intelligent electronic devices (IEDs). Additionally, the use of IEC 61850, IEC 60870-5-104, Modbus TCP, PROFIBUS DP, and HART standard protocols results in reduced wiring and system footprint. Figure 3 below describes the overall architecture of Symphony® Plus.

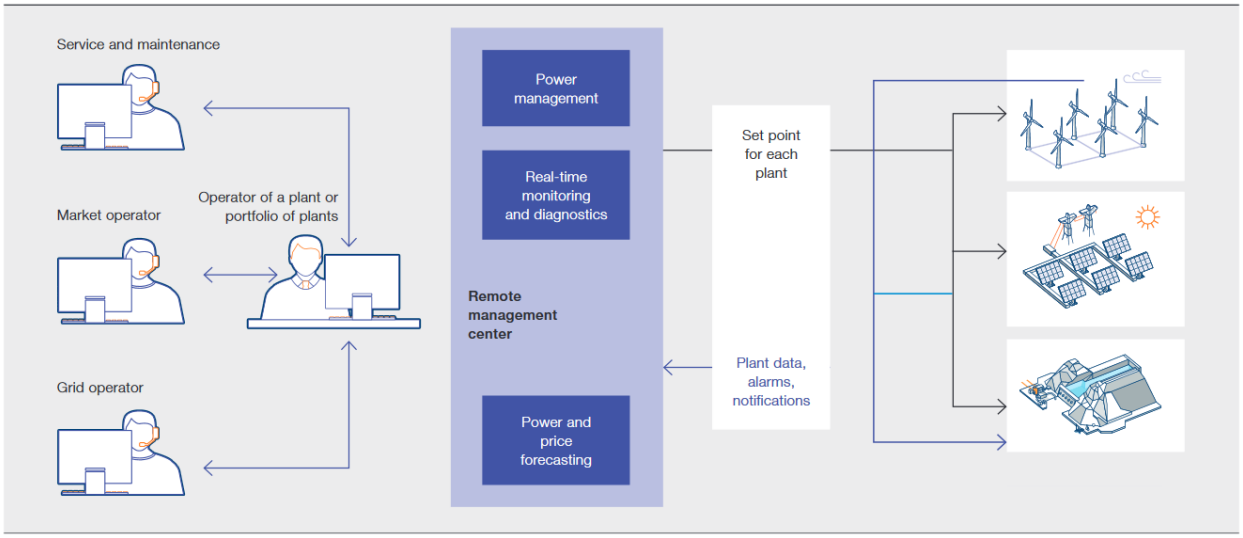

Figure 3. Symphony Plus automation for remote energy management (Timbus & Bitto, 20155)

Another example of SCADA systems in energy applications is renewable energy control rooms, such as that used by Enel Green Power, as sustainable energy company with operations in Chile. (https://www.power-technology.com/features/enels-renewable-energy-control-room/). The operation features a team of 18 on-site engineers, 17 operators, 36 power plants across 2500km of energy grid. The Enel setup includes a control center that centralizes data from SCADA systems, which report status and production level to operators. The operation follows a published standard: Uptime Institute's TIER III standard. One of the main issues discussed in this operation is communication interruptions, for which the solution was redundancy with diverse channels (https://www.powermag.com/control-room-considerations-what-you-need-to-know/)
Automation in SCADA applications has been more recently studied to understand the role of the human operator. Though described as more dynamic and hands-on than automated microreactor concepts, Prostejovsky et al (2019) provide a description of human operators in high-automation electric power systems settings. The paper describes roles, tasks and objectives, expertise levels, and ways of modeling and measuring situation awareness. Moreover, the authors address the changing landscape of human operators in more complex systems as specific types of automation (i.e. machine learning, decision support systems, etc) become more common in the power industry (Figure 4). This paper offers a comprehensive template of considerations for microreactor systems with respect to human-machine interaction.

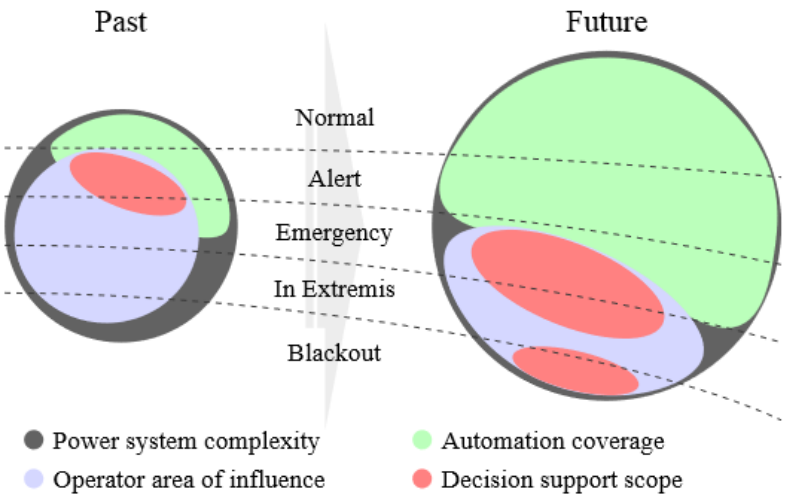

Figure 4. Shift of Influence in Electric Power Systems (Prostejovsky et al., 2019)

Within the United States, entities such as the National Renewable Energy Laboratory (NREL) have started to shift focus to creating more autonomous (and in many cases, modular) systems (https://www.nrel.gov/grid/autonomous-energy.html). However, much of the focus of their work, as advertised on their website, is focused on the development of the technology itself, especially as power grids evolve to incorporate all different manners of energy production using different monitoring, controlling, and distribution methods. That is, NREL's material does not specifically discuss the impact on human operators. If NREL has expertise in understanding impact of technological advancement and evolution on human operators in complex power systems, this is one path that could be pursued in an interdisciplinary effort to address human factors in microreactor applications.

2.2.2. Dynamic Control Systems

The following industry examples different from SCADA systems in the sense that they require continuous monitoring of physical status and position. These dynamic control systems include physical variables to follow or track some desired time function. Examples of dynamic control systems include automotive, aviation, and space applications. Dynamic control systems typically involve a human operator that is expected to maintain some level of control and continuous situation awareness, even though the system might be in control.

2.2.2.1. Space and Earth Orbit Satellites

From a human-computer interaction perspective, satellite monitoring has traditionally been considered a dynamic control system (Mitchell, 1987). Papers in this sub-domain identify a process by which system developers can determine the HMI through functional decomposition of critical tasks for mission success (Russell & Golden, 1996). Within this application segment, there has also been some work to establish requirements for the design and development process of interactive SCADA systems, including scalability, verification, traceability and training (Martinie, Palanque, Navarre, & Barboni, 2012). Other examples of interface design in space applications include

establishing standards for human-robot interfaces (Ferketic et al., 2006; Leidner, Birkenkampf, Lii, & Borst, 2014).

2.2.2.2. Marine, Aerial, and Ground Transportation

Applications that require more dynamic interaction structures often approach human-automation interaction from the perspective of ***human-automation teaming***, indicating more flexible models of control and adaptability (G. L. Calhoun, Ruff, Behymer, & Frost, 2018; Gloria L. Calhoun, Ruff, Behymer, & Mersch, 2017). Moreover, interfaces developed for operators in these settings attempt to incorporate human control of asset allocation, routing, and execution details through system interfaces.

More traditional approaches to function allocation in aerospace applications stem from foundational Human Factors research in the 1950's (Fitts, 1951), which is more generally referred to as "humans are better at – machines are better at", or HABA-MABA. This approach has persisted for more than 60 years (de Winter & Dodou, 2014) is still used in recent examples of Unmanned Aerial Vehicle (UAV) algorithm development (Lin & Goodrich, 2015). There is much research in similar applications for ground transportation (automobiles), which offer a wide array of approaches and areas of focus about human interaction directly with a vehicle during operation (Endsley, 2017; Flemisch et al., 2019; Tenhundfeld et al., 2019)

There is at least one case of a risk model applied to marine environments in order to capture human interaction with autonomous underwater vehicles in the context of mission performance (Thieme & Utne, 2017). Similar to UAVs, unmanned underwater vehicles (UUVs) have contextual factors that impact the efficiency and effectiveness of human-automation teaming in underwater environments, such as interrupted communications and signal transmission. Within human factors research, maritime applications are relatively new with much research being contained within international navies.

2.3. Government Regulations on Human-System Integration

There are several resources regarding human-system integration in the form of standards from different government bodies that oversee different communities. However, many of these standards have not been updated within the last 5 years to accommodate the latest advancements in technology and the potential ramifications on human-systems interaction. Moreover, many of these design standards and documents are context-specific, calling out considerations for specific environments like aerospace, space, military, etc.

The Department of Transportation (DOT) has released some literature regarding human-system integration in the rail industry (DOT/FRA/ORD-18/05), which could be used for microreactor applications. The approach is a combination of adaptations from INCOSE and NASA standards, which generalizes well beyond transportation into general systems design.

Several standards exist specifically for safety of operations in different contexts, though they do not focus solely highly automated systems. Content may need to be extrapolated to automated system safety principles.

- NASA/SP-2010-580: NASA System Safety Handbook (http://everyspec.com/NASA/NASA-SP-PUBS/NASA_SP-2010-580_VER-1_41404/)

- FAA System Safety Handbook: (https://www.faa.gov/regulations_policies/handbooks_manuals/aviation/risk_management/ss_handbook/)
- DOT_J3114_201612: https://www.sae.org/standards/content/j3114_201612/

Several design standards exist to help determine specific elements of system and interface design for different types of controls. MIL-STD-1472G: Department of Defense Design Criteria Standard – Human Engineering (updated 2012) provides comprehensive design guidance for different types of system and include human-system integration-specific applications. This standard is referenced by DOT literature as one of the most comprehensive, with more frequent updates than standards from other industries. Alternatively, the FAA has a standard that provide the same type of information from an aviation perspective [HF-STD-001: FAA Human Factors Design Standard for Acquisition of Commercial-Off-the-Shelf Subsystems, Non-developmental items, Developmental Systems]. Finally, NASA-STD-300: Man-System Integration Standards (https://msis.jsc.nasa.gov/) offers some design considerations that are generalizable to microreactor settings. However, much of the standard is focused on space applications with little detail that could be applied to microreactors specifically.

2.4. Other HFE Considerations

Security is also becoming a very popular topic within the SCADA domain (Macaulay & Singer, 2012). More specifically, vulnerabilities in the system at large, as well as within the HMI (McGrew & Vaughn, 2009), are important to identify and mitigate as the system is developed and deployed. This area is quickly growing to address wider security concerns (Cheung et al., 2006), and even training and education of security operators for SCADA systems (Hahn et al., 2010).

2.5. Summary

There are several industries that have varying degrees of autonomous applications. However, there is relatively low emphasis on explicit human-system integration guidance in the available literature. Moreover, there is a finite distinction between types of systems (i.e. SCADA, dynamic control) that should be acknowledged before modeling future microreactor design from these existing examples. For instance, transportation examples require dynamic control, often with a human operator that needs to maintain high SA, even though he/she might not be physically in control of the system. This is an example of a mid-level of automation that requires high SA, which might fundamentally differ from microreactor system design.

Alternatively, some governance is available from other U.S. government entities regarding safety and human-system integration. These resources should be carefully interpreted, especially as they may not be recently updated to accommodate advances in new technology. However, some of the provided documents do offer comprehensive guidance on certain aspects of human-system integration, which could be helpful in later stages of development and interface design.

3. NUCLEAR REGULATORY COMMISSION GUIDANCE ON HFE

As was stated in Basic Safety Principles for Nuclear Power Plants (75-INSAG-3 Rev 1) and again stated in the Defense in Depth Nuclear Strategy (INSAG-10), "All safety activities, whether organizational, behavioural or equipment related, are subject to layers of overlapping provisions, so that if a failure should occur it would be compensated for or corrected without causing harm to individuals or the public at large." (INSAG, 1999; INSAG, 1996) So, an essential component to designing advanced nuclear reactor facilities is understanding not only the safety activities but also the stakeholders involved in completing those activities.

The Defense in Depth (INSAG, 1996) document reviews the hierarchical deployment of different levels of equipment and procedures to maintain safe operations. Within the Defense in Depth strategy, designers must consider how to prevent accidents and, if prevention fails, limit the potential consequences and prevent any evolution to more serious conditions. Integrating HFE perspectives into this approach means understanding what actions a human can take to prevent accidents and how humans can response to accidents once they've occurred. Further, an understanding of how human actions might cause accidents must also be incorporated within a defensive strategy, so those pathways can be mitigated.

3.1. NRC Human Factors Guidance

Title 10 Code of Federal Regulations (CFR) includes all the requirements for persons and organizations receiving a license from the NRC to use nuclear materials or operate nuclear facilities. Safety inspectors for the NRC must ensure that nuclear facilities are following regulations in operation of their sites. The Standard Review Plan, Part 18 (SRP) (NUREG-0800) provides an overview of the guidance necessary for performing safety reviews of human performance. In this document, the relevant human performance-related CFR requirements, SRP section, and acceptance criteria source material are outlined (NRC, 2016).

Overall, NUREG-0711 "Human Factors Engineering Program Review Model" describes the HFE top-down approach for conducting safety evaluations (O'Hara et al, 2012). This top-down approach describes the HFE elements within the planning and analysis, design, verification and validation, and the implementation and operation of the design. Figure 4 shows the elements of the NRC's HFE program's review model. In completing each element, the nuclear powerplant applicant must submit and Implementation Plan (IP) which describes their proposed methodology for conducting that element. NUREG-0711 explains the review criteria for each and provides a bibliography of source documentation for those criteria.

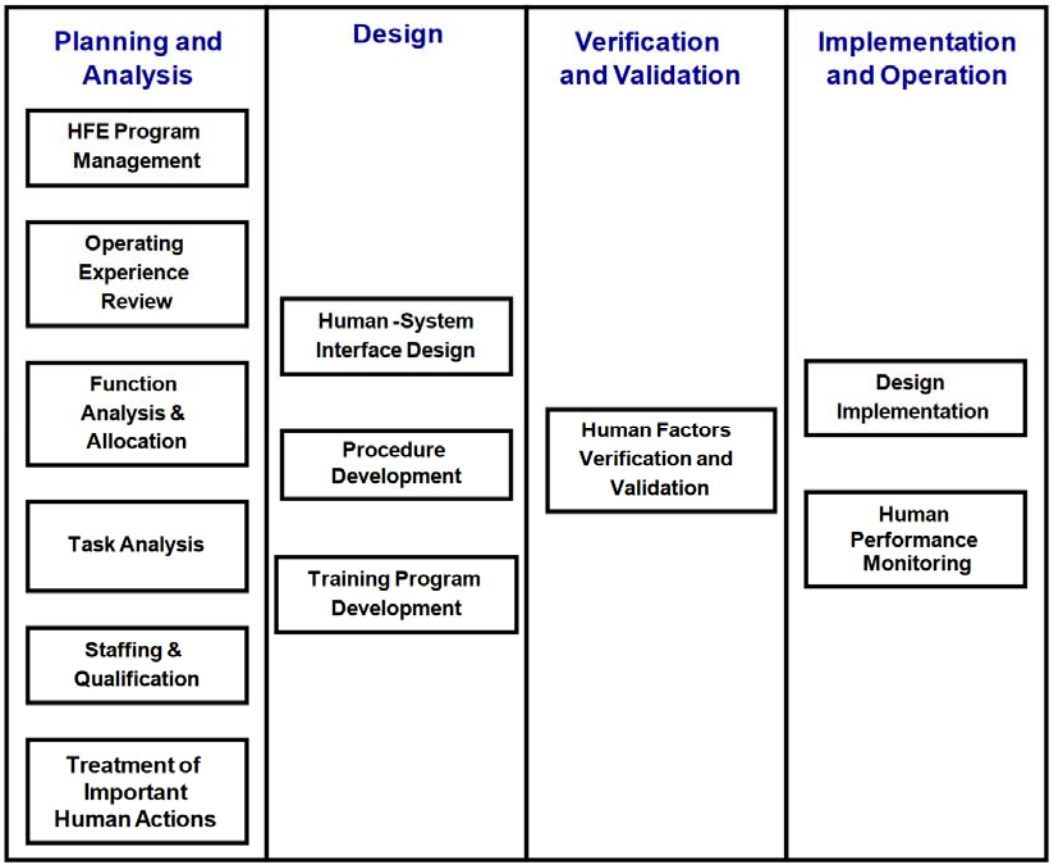

Figure 5. Elements of the NRC's HFE program's review model (NUREG-0711)

3.1.1. Planning and Analysis

3.1.1.1. Operating Experience Review

The operating experience review is required by 10 CFR 52. The operating experience review (OER) is intended to identify HFE-related safety issues in previous designs and ensure that these issues are addressed in a new design (Higgins & Nasta, 1996; O'Hara et al, 2012). The OER should provide information regarding prior NPP designs and safety issues. The output of the OER is used within nearly all the following element of the HFE review process.

For a microreactor, the OER may be difficult to scope since many aspects of the microreactor are new and have limited issues and lessons learned from prior designs for the basis of plant improvements. Past predecessors for microreactors may instead include earlier designs upon which the implemented design is based. However, these designs may not have a clear or quantifiable definition for comparison.

3.1.1.2. Functional Requirements Analysis and Function Allocation

A functional requirements analysis and function allocation are conducted to ensure that the functions necessary to operate the plant are appropriately defined and analyzed (O'Hara et al, 2012). The functions are allocated between human and machine resources to efficiently take advantage of

the strengths of both humans and machines without overtaxing either resource. As was discussed in Section 2, the appropriate level of machine and human engagement must be considered to best meet the plant's goals (Price, Maisano, & Van Cott, 1982; Pulliam et al, 1983; IAEA, 1992)

Within microreactors, a functional decomposition is essential for understanding the expected level of engagement by humans and machines. In the case of remotely run microreactors, the functional decomposition stage of the design process would help in defining the roles and responsibilities of both the humans and machines. Further, the functional hierarchy (Figure 5) could be used to identify critical safety functions and develop requirements for mitigating emergent events.

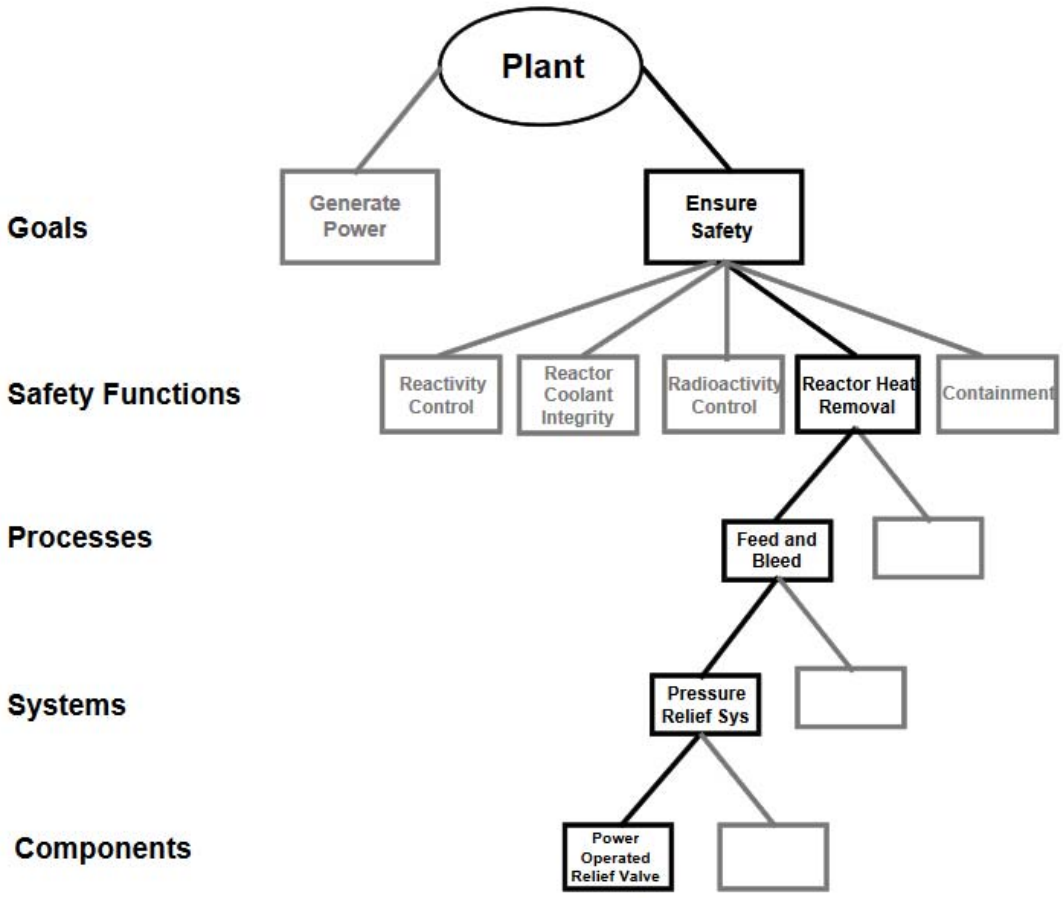

Figure 6. Vertical slice through a plant's functional hierarchy for ensuring safety (NUREG-0711)

3.1.1.3. Task analysis

Once a plant's functional hierarchy has been decomposed, an applicant must then assign specific tasks to human personnel as well as the necessary information, control, and task support for completing the tasks (O'Hara et al, 2012). For the NPP task analysis, applicants are to provide a description of: personnel tasks; relationship between tasks; a time estimate; workload estimate; alarms, information, controls, task support necessary; number of personnel; and the necessary knowledge and abilities. Further, these tasks should be representative of a full range of plant operating modes (e.g. startup, normal operations, low-power and shutdown conditions, transient conditions, abnormal conditions, emergency conditions, and severe accident conditions).

For microreactor facilities, human tasks may shift depending on their level of involvement in day-to-day operations. Since operators may be expected to supervise multiple microreactors via a remote site, the task analysis would need to consider the increased workload required by monitoring multiple reactors. The task analysis would also need to consider the information necessary for supervising the multiple microreactors. Within the analysis of plant operating modes, the applicant would need to be aware of the full range of modes that are possible with a microreactor plant. Are the current recommended operating modes applicable for these newer reactors? Or, do other modes need to be considered?

3.1.1.4. Staffing and Qualifications

The required minimum number of personnel and their expected tasks are defined in the task analysis from the previous HFE element (O'Hara et al, 2012). The specific staffing levels and qualifications are highlighted in a separate section of the license application. Within this section, the licensee must be able to demonstrate how the staffing levels and qualifications were determined and validate that the staffing levels are appropriate.

Currently, 10 CFR 50.54 provides a minimum number of onsite staff. However, this number may not be appropriate for microreactor personnel. Within the current application framework, an applicant would need to submit an exemption to deter from the regulatory standard (NRC, 2005). Thus, future regulatory guidance may need to provide flexibility for licensees to define their own staffing levels as determined by their validated analysis.

3.1.1.5. Treatment of Important Human Actions

Human actions that are most important to safety are identified using a combination of probabilistic and deterministic analyses (O'Hara et al, 2012). As an example of probabilistic analyses, a probabilistic risk analysis, including an human reliability analysis (HRA), estimates risk by evaluating: What can happen; how likely is it to happen; and given that it occurs, what are the consequences? (Bedford & Cooke, 2001) An HRA similarly evaluates contributions to risk made by human failures (Reason, 1990). The PRA and HRA are initiated early within the design process so that designers can gain insights about how the design can be improved and about how HFE considerations may impact plant outcomes (Kolaczkowski et al, 2005). Through these assessments, important human actions can be identified. A final safety analysis report/design control document deterministic analysis is also performed and used to similarly identify important human actions. Figure 7 outlines how these analyses are included within the plant design process.

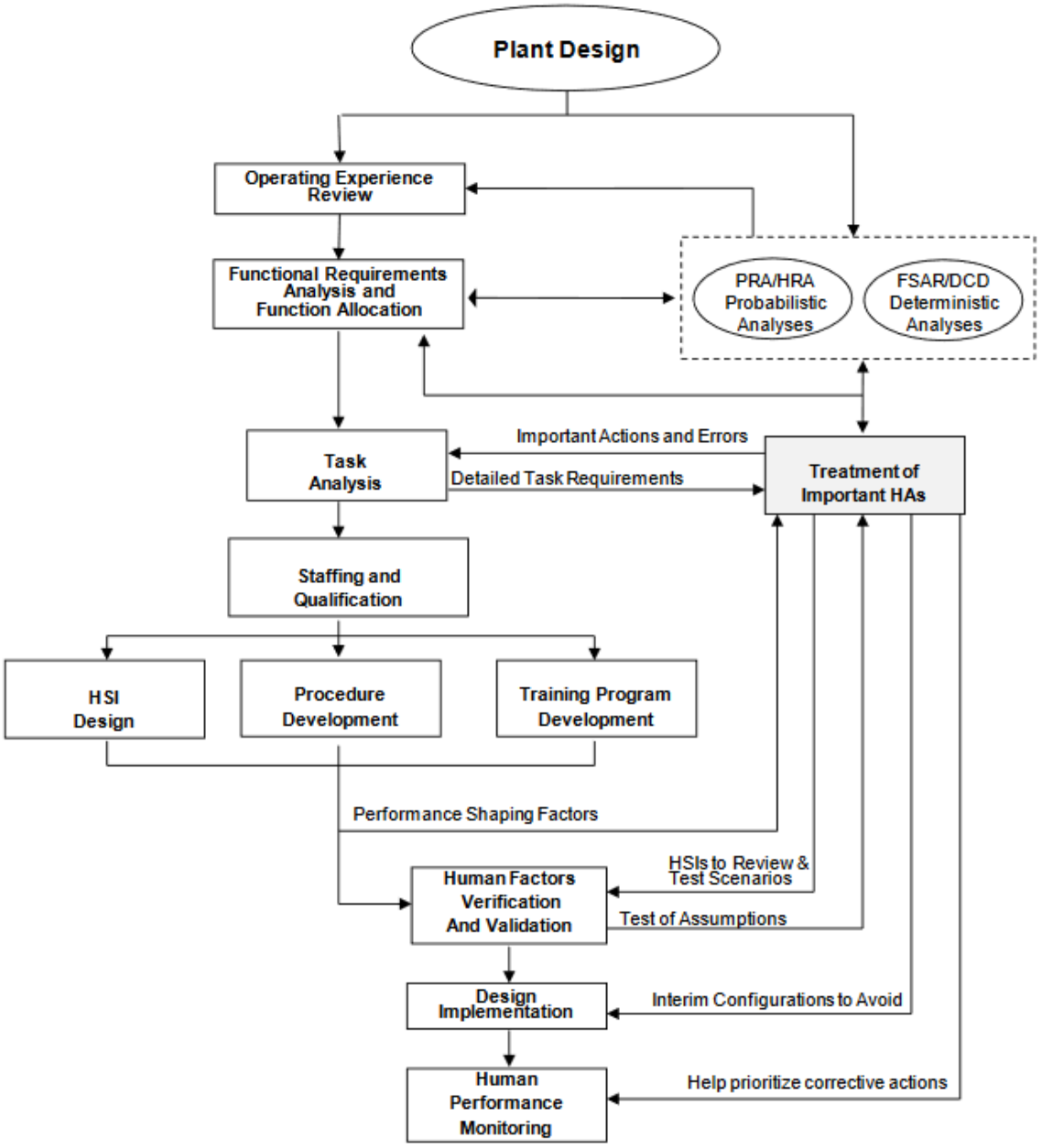

Figure 7. The role of important human actions in the HFE program (NUREG-0711)

For microreactors, a probabilistic risk assessment (PRA) and HRA would need to be completed for the novel control room design. The analyses would need to assess the need for physical human intervention onsite in the event of an emergency or off-nominal situation. The length of time necessary for plant stabilization before human intervention is required would need to be highlighted within the risk assessment.

3.1.2. Design

3.1.2.1. Human-Machine Interface Design

The HMI is designed using a structured methodology and the resulting design is evaluated using user input (O'Hara et al, 2012). Changes to the design should be made earlier in the design process to minimize cost and difficulty, which can become an issue for later design phases. In creating an HMI, licensees must describe how personnel interact with the system as well as a detailed description of the HMI design. The resulting HMI must be compared to the previous HFE elements to show a validated design process. NUREG-0700 outlines the design guidelines for interfaces, including information display, user-interface interaction and management, and control (O'Hara et al, 2002). While NUREG-0700 and NUREG-0711 provide very detailed guidance on specific aspects of current NPP facilities, this guidance may not be applicable for microreactor operator interactions (O'Hara et al, 2002; O'Hara et al, 2012). The current guidance provides criteria for design of the Main Control Room, Technical Support Center, Emergency Operations Facility, Remote Shutdown Facility, and the Local Control Stations. These spaces may not be included in the same manner, if at all, in microreactors.

3.1.2.2. Procedures

Procedures support and guide personnel interactions with plant systems and personnel responses to plant-related events (O'Hara et al, 2012). Within nuclear power plants, an individual utility is responsible for developing their procedures. These procedures are then reviewed by the NRC. For new plants, such as microreactors, the procedure development is supported by the analyses performed throughout all HFE elements (NRC, 1982).

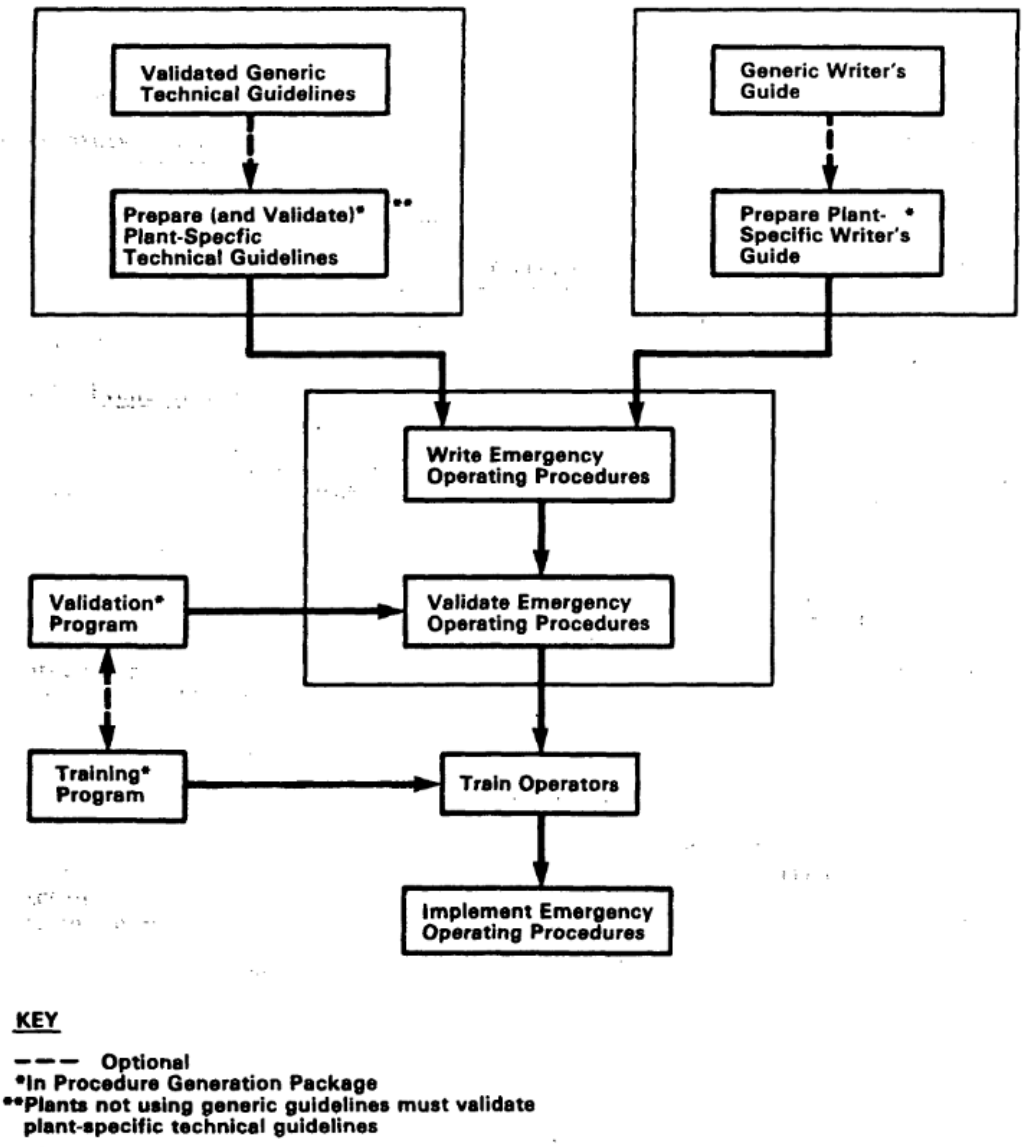

Figure 8. Sample program for developing emergency operating procedures (NUREG-0899)

3.1.2.3. Training

Training is a critical component of successful HFE design, and must be developed through coordination with the other elements within the HFE design process (O'Hara et al, 2012). The knowledge, skills, and abilities personnel need to successfully meet plant goals are defined through the job and task requirements. Similar to the procedure development, training programs are the responsibility of the utilities, reviewed by the NRC. To develop the training, a systematic analysis of the tasks and jobs to be performed can give insights to the specific learning objectives necessary to achieve a desired performance (NRC, 1993). There must also be an approach to evaluating mastery of the knowledge, skills, and abilities after completing the training course.

Within advanced reactors, such as microreactors, any HFE analysis performed by the vendors should be integrated into the training program design. Since microreactors may have more passive

safety features and operators may be located remotely, this may reduce certain types of training needs while increasing other training needs. For example, NUREG-1122 and NUREG-1123 provide the knowledge and abilities catalogue for NPP operators of Pressurized Water Reactors and Boiling Water Reactors (NRC, 1998; NRC, 2007). This knowledge set may not be applicable for microreactors. Since the operators may be located remotely and have fewer interactions with the plant controls, operators' knowledge and ability requirements may have a smaller catalogue than current standards.

In future training programs, utilities can use simulator scenario-based testing methods. This would allow for the evaluation of operators in a low-risk environment while still providing them with hands-on experiences (NRC, 2011)

3.1.3. Verification & Validation

The Verification & Validation (V&V) task evaluates the integrated system for HFE design conformity and cohesive integration with plant personnel requirements (O'Hara et al, 2012). The review looks back at previous phases of the HFE design process to verify that the interface supports personnel's tasks as defined by the task analysis (Task Support Verification) and that the interface accommodates for human capabilities and limitations (HFE Design Verification). The integrated system's design is validated through an Integrated System Validation (ISV). The ISV evaluates whether the design meets performance requirements and supports the plant's safe operation.

3.1.4. Implementation & Operation

3.1.4.1. Design Implementation

The design implementation addresses both the installation and the testing of the final design. The applicant is expected to ensure that the planned design matches the actual design as it is fielded (O'Hara et al, 2012).

3.1.4.2. Human Performance Monitoring

Human performance monitoring provides assurance that the careful inclusion of HFE considerations throughout the design process is maintained in plant operations over time (O'Hara et al, 2012). Specifically, the NRC is concerned about performance degradation over time, whether due to attrition or due to changes made in the plant.

4. MICROREACTOR AUTOMATION IMPLICATIONS TO SAFETY

A passive safety system is one for which there is no reliance on such external inputs to achieve the desired safety function. In a passive safety system, the safety function is achieved through reliance on laws of nature, material properties, and energy stored within the safety systems, structures, or components (SSC). Passive safety within microreactor design is intended to ensure that the reactor will fail-safe and be self-regulating. Additionally, the reactors are expected to be less complex with less active components. While the previous sections discussed human factors considerations in the context of nuclear power plant design, this section transitions to discuss the context of interest: microreactors. The first part of this section discusses a semi-structured interview with subject matter experts working with microreactors. The second part of this section discusses "inherent safety" in more detail. And, the third part of this section discusses how humans are expected to be incorporated within microreactors.

4.1. Subject Matter Expert Interviews

In November 2019, three semi-structured interviews were conducted with five subject matter experts (SME) working on advanced reactor concepts. Two of the interviews had one SME, and the third interview had three SMEs from the same organization. The participants work at NRC, Electric Power Research Institute (EPRI), and Los Alamos National Laboratory (LANL), and all the participants work in a varying capacity on advanced reactor design and/or regulation. The purpose behind the interviews was to gain insights on the direction of microreactor design and implications to human reliability and safety from a variety of stakeholders in the microreactor design process. Appendix A has a complete list of the questions that were included in the interviews, and Appendix B has the notes that were taken during the discussions.

The NRC SMEs work in the Office of Research and Human Reliability and the Office of New Reactor Regulation. The individual from EPRI has worked on risk assessment in the past and now works on research-based nuclear reactor projects, including research into microreactors. And, the individual at LANL is a project lead on a current microreactor development project. Each SME contributed their perspective on current research directions and future design implications of microreactor research and design.

Overall, the experts had a common agreement that the microreactor field is moving more toward autonomous designs. From the conversations, the experts conveyed that current regulations, while based on large-scale reactor designs, may be too prescriptive and not appropriate for microreactor operations. Further, the level of autonomy within the microreactor design may vary by type, with some being recommended for full autonomous operations and others having more remote operator interactions. There may also be a difference in passive safety features versus active control features. With the movement toward an autonomous reactor design, the human operators are likely to take on a more monitoring role, with some human-driven inputs required to adjust the power output if needed.

While the SME's agreed that microreactors are moving toward more autonomous operations, they had disparate perspectives on the overall impact of microreactors to their surrounding environment. This perspective was evident in the assumptions regarding inherent or passive safety within the design via a passive control system. Some of the SME's conveyed that they are optimistic that the reactors will be able to be unmanned outside of nominal maintenance operations. However, they all recognize that this will make software design and certification an essential component of

microreactor design implementation. If remote monitoring is expected within the operation of the facility then remote sensors are also important to microreactor design implementation.

In the event of an emergent situation, there were mixed expectations regarding the need for immediate human response to control the situation and prevent radiation release. Some microreactor designs have published standards lengths of time that a reactor should be considered "safe" if an event were to occur. These times are discussed in the next section. Additionally, the amount of possible radiation that can be released to the surrounding environment is much lower than that of light water reactor facilities. Therefore, the emergency planning zone (the area that would be impacted by nuclear exposure) will be smaller surrounding the microreactor facilities. However, this may be influenced by the specific installation location. The impact on the surrounding area will be different if the microreactor is in an extremely remote region with no neighboring humans as opposed to the installation of a facility in a metropolitan area or on a military base.

Overall, the SME's all had a similar statement regarding the creation of NRC regulations for licensing microreactor facilities: Regulations should incorporate a spectrum of guidance for varying levels of automation and human involvement. That is, the vendors currently designing microreactor facilities are each taking their own unique approach to reactor design, and NRC regulations must account for the variability between designs while also ensuring safety at each site. Human involvement within each type of microreactor facility varies depending on the robustness of the design's passive safety features. Sites also vary in their frequency of scheduled onsite maintenance activities which would involve a human maintainer.

4.2. Inherent Safety in Microreactor Designs

Consideration of the risk profile (and safety) for a microreactor requires evaluation of a number of significant changes in the design philosophy behind how fundamental safety functions are provided. In previous generations of water-moderated reactors, SSCs that maintained control, cooling and containment of radionuclides were generally designed in a manner that they could be considered active SSCs. An active SSC relies on external mechanical and/or electrical power, signals or forces (IAEA, 2018).

By contrast a passive safety system is one for which there is no reliance on such external inputs to achieve the desired safety function. In a passive safety system, the safety function is achieved through reliance on laws of nature, material properties, and energy stored within the SSC. As a result, the typical causes of failure for active systems generally do not exist for a passive system—i.e., loss of power or failure of operator action. By contrast, passive systems can fail as a result of modes such as mechanical or structural failure of an SSC, or even malicious human intervention (IAEA, 2018).

Other considerations are also relevant for assessing the reliability of passive safety systems. For example, passive cooling systems typically rely on natural circulation flows to transport heat to an ultimate heat sink. These natural circulation flows rely on small pressure gradients in the fluid that drive small flows. As a result, these circulation patterns can be susceptible to breakdown should these gradients be eroded. For example, a small reduction of heat transfer to the ultimate heat sink could lead to a breakdown of a natural circulation pattern. As a result, the overall reliability of a passive system can depend sensitively on how the governing physical process is influenced by boundary conditions.

The characterization of these boundary conditions across a range of upset conditions can be generally difficult to assess. However, a passive safety system is designed to maintain relatively controlled boundary conditions that ensure it will function to control a plant under a broad range of internally initiated upset conditions. Passive safety systems are thus very reliable when considering the provision of their safety function to defend against internal events. An active system, by contrast, has a much higher probability of failing randomly when called upon to perform its safety function.

A passive safety system is more difficult to characterize when considering the impact of an external event. For example, does a seismic event, leading to structural failures that cause cooling fins to be dislodged from a heat exchanging structure, cause a sufficient degradation in heat transfer that the passive heat removal function fails? This requires a broader understanding of how the physical processes underlying the passive safety function perform under a broad range of degraded conditions induced by the perturbing external event.

In contrast to passive safety, inherently safe systems are those which are absolutely reliable. The classification of absolute reliability must be qualified by a detailed consideration of the range of characteristics of the SSC that support the safety function. For example, control of reactivity often involves reactivity feedback mechanisms inherent to a system preventing reactivity excursions from occurring (e.g., moderator temperature feedback). In this case, it is generally difficult to postulate an external perturbation that would give rise to a loss of reactivity control. However, for cooling or containment functions, it is more likely that passive systems can exhibit failures under a range of external perturbations such that they are not absolutely reliable. Under some circumstances, however, even cooling functions may be ultimately reliable should the power level of the reactor be sufficiently low that residual heat can always be rejected to the atmosphere.

For the purposes of assessing the role of human interventions in preserving function of passive safety systems (including those that are absolutely reliable), the following considerations are relevant.

- **Human intervention generally not required**: Boundary conditions of the passive safety system do not practically change—for example, an atmospheric heat sink can serve as an infinite reservoir for residual heat from the fuel. In this case, it is reasonable that very limited to no on-site response would be required to ensure the function is preserved. In addition, no off-site staging would need to be ready to be called upon to transport and implement the means to restore the safety function.
- **Human intervention required in the long-term**: Boundary conditions of a passive safety system evolve very slowly with time such that significant time exists for intervention to implement recovery measures that either maintain the passive safety system or replace it with an alternate system to maintain the safety function. In this case, there is likely no need for on-site operations to be available to preserve this safety function. Sufficient time would exist for the transport of operators and equipment to either restore the passive safety system or implement an alternate system to maintain the safety function.
- **Human intervention required in the medium-term**: Boundary conditions of a passive safety system evolve somewhat slowly such that the passive safety system can remain operational for a period of time. This operation time is sufficient for on-site operators, using equipment staged on-site, to implement measures that either preserve the operation of the passive safety system or replace it with an alternate system. In this case, the degradation of the passive safety system occurs too quickly for off-site operational personnel and equipment to be transported to the

microreactor installation to preserve the passive safety system or replace it with an alternative system.

- **Human intervention required in the short-term**: Boundary conditions that maintain the operation of the passive safety system within its design envelope degrade rapidly. In this situation, loss of safety function occurs so rapidly that there would be no time to implement an alternate system to maintain the safety function. In this situation, operator intervention would be required in a time sooner than that over which an alternate system could be implemented to maintain the safety function. In this case, the operators must be trained to perform functions over a relatively short time period to preserve the function of the installed passive safety system. There is likely limited time to stage and implement additional equipment stored on-site. Any additional equipment would likely be required to be located where operational staff are required to perform the necessary operations.

The range of operator interventions considered above are influenced by the following parameters

- Minimum time when action is required to preserve the safety function
- Complexity of the action to preserve the safety function

The complexity of the action is partially dependent on the time over which action is required. Generally, the complexity of the operation can increase with the more time required to act. For example, transport of equipment from off-site locations to the microreactor facility involves a number of complex operations.

The time frames considered above have been introduced as qualitative bins. Industry guidance does exist that has established reasonable estimates for these time bins. Based on the FLEX guidance developed post-Fukushima (NEI, 2016)

- Long-term times are on the order of about 24 hours: On-site equipment should be capable of performing the safety function for a minimum of 24 hours; that is, off-site equipment is assumed to become available after at least 24 hours. Depending on the location of the microreactor facility, the time to bring off-site equipment and personnel to the site may be considerably longer. This could be the case for remote installation. However, based on FLEX guidance, long-term time frames can be established based on the time required to transport personnel and equipment to the site.
- Medium-term time frames are on the order of a few hours after augmented staff can arrive on-site: Typically, a few hours are required for augmented staff to perform the necessary actions after arriving on-site. The FLEX guidance indicates that transition of safety functions to alternate means established with on-site equipment is about 8 hours, given that augmented staff will start to arrive on-site by 6 hours. Based on this guidance, one choice for the medium-term time frame is a few hours after augmented staff can arrive on-site to preserve the passive safety system or implement alternate systems. However, should the complexity of the actions or other operations required be relatively low, it is reasonable that medium-term involves only the few hours required to implement the action because on-site personnel could readily perform the action.
- Short-term time frames are typically required shortly after the event to preserve operation of the installed passive safety system. These actions must be able to preserve operation of the passive safety system for a sufficiently long time to enable actions taken in the medium-term to be implemented. As a result, any short-term action by necessity must have relatively minimal complexity.

While behaviors required to perform the action can affect the definition of the above time bins (i.e., the time required to perform the action), it has additional implications. For relatively simple systems such as is the case in proposed microreactors, possible actions to manage an event may be relatively simple. Such actions generally do not require the same level of training.

For effective training design and human behavior attainment, a designer must identify the desired level of performance. Figure 9, copied from Rasmussen (1983), illustrates these three levels, which are described as skill-based, rule-based, and knowledge-based behaviors. The level and depth of training can vary based on the desired attainment of "skills, rules, and knowledge" (SRK) from the human learner (Fleming, 2013; Fleming & Pritchett, 2015; Ivergard & Hunt, 2009).

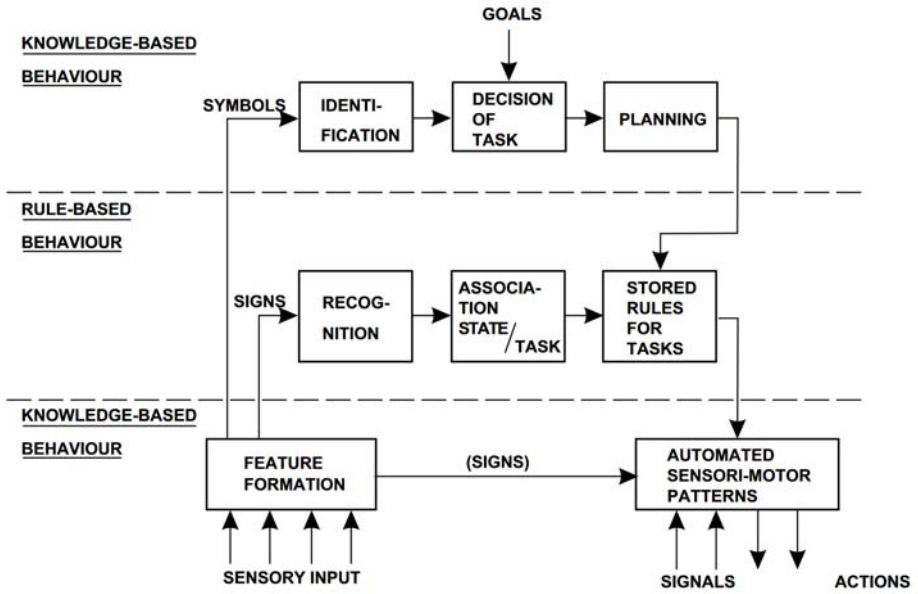

Figure 9. Skill-based, rule-based, and knowledge-based behavior (Rasmussen, 1983)

Skill-based behavior represents human performance that does not need conscious control. The human can sense a sign and automatically perform the task based on a simple feedback control. This behavior optimizes human motor skills and needs feedback relative to acceptable performance boundaries (Rasmussen, 1983; Rasmussen & Vincente, 1989).

Rule-based behavior denotes recognition of a sign or cue and the subsequent performance of a stored rule or procedure. The performance of tasks using rule-based behaviors are goal based, and the rules for task completion are formulated from previous occasions experienced in training or real operations (Rasmussen, 1983; Rasmussen & Vincente, 1989).

Knowledge-based behavior corresponds to situations when higher level cognitive skills are used, and decisions are made by incorporating an analysis of the environment and symbols contained within. Frequently, tasks performed using knowledge-based behaviors take longer to execute, as the human is actively searching for information in novel situations (Rasmussen, 1983).

Required SRK may vary in microreactor operations depending on the human actions required for both nominal situations as well as off-nominal, emergent situations. For nominal situations, the human operators are likely trained to follow mostly skill-based and rule-based behaviors. Training for typical events would focus on the operator understanding and following a defined set of procedures with occasional knowledge-based behaviors if the human needed to interpret a reactor

output and adjust their procedures accordingly. For off-nominal situations, a human operator may need additional training to follow emergency procedures. Emergency situations may also present novel situations, causing human operators to rely on knowledge-based behaviors. They may need to analyze the environment and perform subsequent tasks based on the environmental context. Training for emergency events should not only discuss the relevant procedures, but also highlight important environmental cues for the operator to use in their situational assessment and consequent response.

4.3. Small Modular Reactor Designs and Planned HFE

Within current nuclear power plant operations, humans take on many roles at onsite facilities. These roles may include operator, maintainer, security personnel, leadership, as well as many other roles within the facility. Each role includes a variety of responsibilities for ensuring safe, secure, and reliable operation of the power facility. At newer, microreactor facilities, the roles may be compressed, shifted, or even eliminated depending on the needs for ensuring operations are maintained in both nominal and off-nominal situations. While Small Modular Reactors (SMRs) are expected to produce a larger amount of energy (50 to 300 megawatts compared to 1 to 50 megawatts), the expected design features of an SMR are similar to microreactor designs. Both reactor concepts will likely make increased use of systems based on passive or inherent safety, be adaptable to a range of energy demand scenarios, and will likely be relatively simpler to operate than the current generation of large LWRs. Some designers for SMRs have released information regarding how they might expect humans to interact within their facilities and at what intervals (Sowder & Marciulescu, 2016). The plans for SMRs may provide insights for even further staffing reductions being contemplated for microreactors.

Babcock & Wilcox Technologies (BWXT) mPower has a fuel cycle of 4 years, is designed for safe shutdown after design basis accident without operator intervention for at least 72 hours, and a 14 day coping time without offsite or onsite AC power. Therefore, the mPower needs little onsite human intervention.

The NuScale Power Module (NPM) has eliminated the need for reactor coolant pumps (less moving hardware) and can enter safe shutdown with no operator intervention. For emergency cooling, the NPM has a few safety-related valves. However, if AC power is lost, a below-ground pool serves as an intermediate heat sink. Hence, the NPM also requires little onsite human intervention.

The Holtec Inherently-Safe Modular Underground Reactor (HI-SMUR SMR-160) intentionally eliminated many active systems and components, relying on natural circulation and containing no reactor coolant pumps. Holtec reports a simplified design with passive cooling for the associated spent fuel pool. The Holtec SMR-160 also requires little onsite human intervention.

The Westinghouse Small Modular Reactor (W-SMR) is more evolutionary than the other designs. The W-SMR balances leveraging current licensing regulations and construction/operation/maintenance experience at the expense of a more passive safety system and overall design simplification. The W-SMR continues to use reactor cooling pumps and AC power for forced reactor coolant flow. Core replacement occurs on a 24-month cycle. While some passive safety was sacrificed, the W-SMR offers defense in depth for passive decay heat removal via a gravity fed cooling water, passive heat exchanges and use of bleed and feed methods. The plant safety systems do not require ASC power and the plant can provide safe shutdown for seven days before additional water is needed. Due to the incorporation of a more complex design, the W-SMR does require more human monitoring and interaction than other American SMR systems.

4.3.1. NuScale ConOps

Recently, NuScale Power, LLC published a Concept of Operations (ConOps) for the NuScale 12 unit plant design (NuScale Power, 2019). The ConOps "describes how the design, systems, and operational characteristics of the plant relate to the organizational structure, staffing, and management framework." (NuScale Power, 2019) The ConOps follows NUREG-0711, which was described in Section 3 of this report. The ConOps defines their staff size at six licensed operators: three reactor operators (ROs) and three senior reactor operators (SROs). The SROs are compressing multiple roles into their position, including shift manager, control room supervisor, and shift technical advisor. The human operators share roles with the machine agent. The machine can vary its level of automation, from fully automated to manual assist. When the automation is used to perform a task the human monitor's its completion. The ConOps continues to discuss the tasks required of the operators as well as the layout of the workstations, interface layout, and features to support human performance.

4.4. Gaps in Understanding HFE in Microreactors

The task analysis and risk assessment methods presented within NUREG-0711 are targeted toward manual human actions and errors. However, operators within the microreactor context may not perform many (if any) manual actions. Instead, they will likely be engaging with a cyber system and remotely controlling microreactor operations. Additionally, the operators may be working with a SCADA system rather than a single control room layout, as was presented in the NuScale ConOps. An approach may need to be developed to design a control room for SCADA interactions and evaluate operator performance in remote monitoring tasks.

Additionally, future microreactor ConOps should provide rich detail regarding specific design metrics used within the HFE plan. Supporting evidence should be presented to validate decisions made around the level of automation within a microreactor control facility. Safety scenarios should be presented demonstrating the robustness of microreactor facilities to a range of off-nominal conditions.

5. APPROACH FOR DESIGNING AND REGULATING MICROREACTORS

The following section outlines recommended steps for designing and regulating microreactors from the perspective of safe and effective human operation. The respective steps, described in detail below, include:

1) Define the concept of operations of microreactors to help capture user/operator perspectives
2) Define the functional architecture of the system, including different aspects of operation
3) Explicitly define human intervention; understand safety implications and requirements
4) Determine appropriate level of automation, alternatively human operator level of control
5) Determine interface requirements to support human operator across system states

5.1. Define the Concept of Operations (ConOps)

The first step of designing a new system after operational needs have been identified is to develop a concept of operations. A Concept of Operations (ConOps) is an enterprise-level living document that helps define a conceptual view of a new system, particularly from the perspective of the user/operator. The ConOps indicates assumptions and intent of the system and can also act as a justification for why the system should exist (the need), how it meets stakeholder needs, the requirements that ensure those needs are met, as well as lifecycle information of the entire system. Additional objectives of a ConOps include (MITRE, n.d.):

- Establish a high-level basis for requirements that supports the system over its life cycle.
- Establish a high-level basis for test planning and system-level test requirements.
- Support the generation of use cases to test the interaction points within the system.
- Provide the basis for computation of system capacity.
- Validate and discover implicit requirements.

Systems engineering literature provides a myriad of resources for developing a ConOps. (ANSI/AIAA, 2012; Blanchard & Fabrycky, 2006; "IEEE Guide for Information Technology - System Definition - Concept of Operations (ConOps) Document (1362-1998)," 1998; Kossiakoff & Sweet, 2003; Levis & Wagenhals, 2000) are excellent resources for developing a solid set of documentation around system architecture. Note that these documents usually involve a wide set of stakeholders as sources of inputs; this helps manage expectations and outputs.

One outcome of the ConOps is to have a clear perspective of the user/operator. Though fine detail of the user/operator role may not be defined at this stage of conceptual development, it is important to have some vision or expectation for what is desired. This helps capture potential scope of user activity, system states and corresponding user interactions, and use cases/scenarios to help drive HMI development.

In constructing the ConOps, some of the necessary document components have already been identified in other activities under this project. SME interviews conducted as part of this literature review provide valuable insights regarding additional work that is needed to determine and integrate stakeholder inputs. These directly inform the system goal and stakeholder needs. Additionally, the

NuScale ConOps provides some direction regarding how other manufacturers have defined the overall system https://www.nrc.gov/docs/ML1913/ML19133A293.pdf

- https://inldigitallibrary.inl.gov/sites/sti/sti/6899532.pdf

While the ConOps offers a high-level view and justification for a new system, the next stage of system development aims to define more specific concepts of lower-level systems that address user needs. These concepts describe specific problems, the operator's viewpoint, intended behaviors, bases for verification and validation activities, basis for number of units, availability, deployment locations, and basis for evaluation of future changes (ANSI/AIAA, 2012). The development of these specific components embodies the transition from a lower fidelity to mid-level fidelity system concept, which grow and mature throughout the product lifecycle. Accordingly, this transition should include definition of measures of effectiveness of the new system.

This document should provide a forum to "stimulate information exchange at the *operational level* on major technical and programmatic issues among the system's users, operators, and developers in order to facilitate clear understanding of the system context and the users' view of the completed system" (ANSI/AIAA, 2012, p. 12). More importantly, this document should precede system specification, as it will provide key inputs to system requirements analysis and design. Finally, operational concepts can and should be applied at lower levels of the overall system hierarchy and developed concurrently with system requirements.

5.2. Define System Architecture

In order to properly scope the human-automation interaction with the future microreactor system, it is necessary to create a preliminary functional system architecture that will help define:

- What will the system do?
- How does that need to be managed?
- What are the expected states of the system?

There are many different approaches to developing system architectures, many of which come from Systems Engineering and related literature. (Levis & Wagenhals, 2000) provide a framework for developing functional architecture. Figure 10 and Figure 11, below from (Levis & Wagenhals, 2000), depict the phase of functional architecture within the larger development process and the necessary components to define critical aspects of the system.

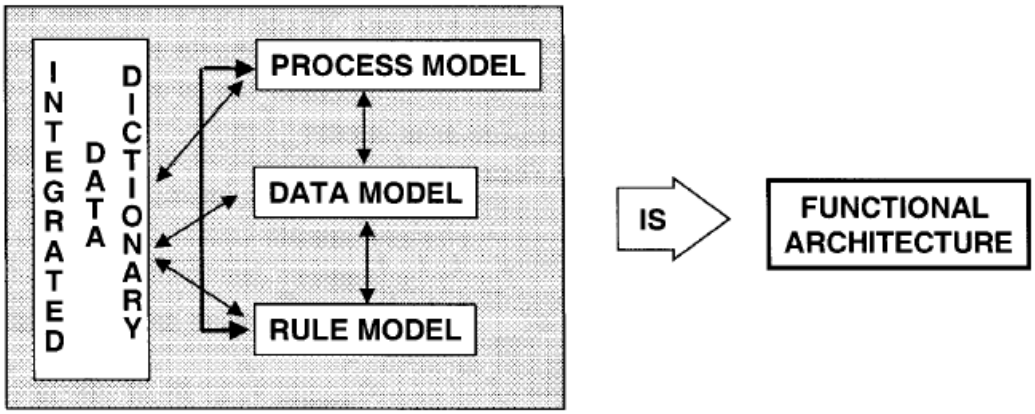

Figure 10. Components of functional architecture (Levis & Wagenhals, 2000)

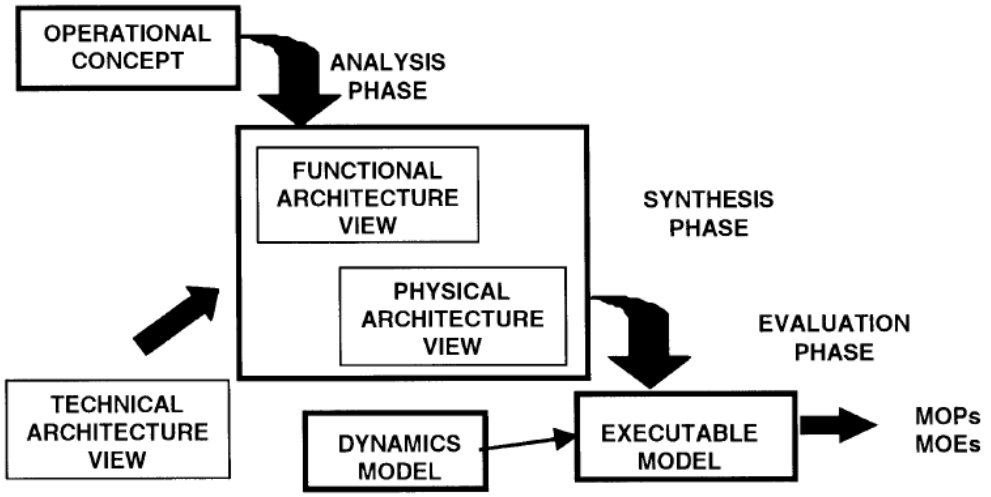

Figure 11. Three phases of architecture development (Levis & Wagenhals, 2000)

5.3. Define Human Intervention / Control & Level of Automation

With a developed concept of how the system will function (functional architecture), it is possible to then determine where the human controller plays a role in system operation. The expected states of the system help define these responsibilities and expectations around what inputs and outputs might be needed in order for those states to be reached or managed. The following steps help define specific points of human intervention and control, and the respective level of automation for each point. These steps can be considered iterative to ensure coverage and integration of changes into prior analysis.

5.3.1. Define Human Intervention and Control

As described in Section 2.1.1., function allocation is the process of assigning activities between a human operator and technology. Despite its pervasive emphasis in Human Factors and Systems Engineering processes, function allocation literature lacks specific methodologies. Fuld (2000) has criticized the concept accordingly, and identified specific methods that provide the desired outputs of function allocation such as functional decomposition as an *a priori* method or task analysis.

Function allocation is more difficult in practice, with few methodologies to support robust assignment (Fuld, 1993, 2000; Wright, Dearden, & Fields, 1999). Despite NRC guidance on function allocation in NPPs (Table 1 below), Fuld (2000) has identified that function allocation may not be robust enough by itself to identify potential errors in allocation via hazards that occur in post-design operation. It is recommended that two methods are used to support the function allocation activity, both of which support identifying potential hazards in complex systems and determining reliability of human operators. Richer representations of work, such as models in contextual design (Holtzblatt, 2016; Holtzblatt & Jones, 1993), offer useful insights in practice (Wright et al., 1999).

Table 1. Human/Machine Capabilities from NUREG-0700, 1981 (Fuld, 2000)

Humand excel in	Machines excel in
Detection of certain forms of very low energy levels	Monitoring (both personnel and equipment)
Sensitivity to an extremely wide variety of stimuli	Performing routine, repetitive or very precise operations
Perceiving patterns and making generalizations about them	Responding very quickly to control signals
Detecting signals in high noise levels	Exerting great force, smoothly and with precision
Ability to store large amounts of information for long periods—and recalling relevant facts at appropriate moments	Storing and recalling large amounts of information in short time periods
Ability to exercise judgement where events cannot be completely defined	Performing complex and rapid computations with high accuracy
Improvising and adopting flexible procedures	Sensitivity to stimuli beyond the range of human sensitivity (infrared, radio waves, etc.)
Ability to react to unexpected low-probability events	Doing many different things at one time
Applying originality in solving problems: i.e. alternative solutions	Deductive processes
Ability to profit from experience and alter the course of action	Insensitivity to extraneous factors
Ability to perform fine manipulation, especially where misalignment appears unexpectedly	Ability to repeat opertions very rapidly, continuously and precisely the same way over long periods
Ability to continue to perform when overloaded	Operating in environments which are hostile to humans or beyond human tolerance
Ability to reason inductively	

5.3.1.1. System-Theoretic Process Analysis

System-Theoretic Process Analysis (STPA) offers a robust approach to identifying this element of system design (Leveson & Thomas, 2018). STPA specifically helps identify hazards within a given control structure, which closely aligns with the goal of the HFE team on this project. STPA, like the systems architecting methodology, starts with a functional model of the system (as opposed to physical), creating some advantage in that the 'form' of the system does not need to exist yet. Essentially, STPA can be used in earlier stages of development as opposed to traditional fault tree modeling. Rather, the intended control structure is the basis for analysis.

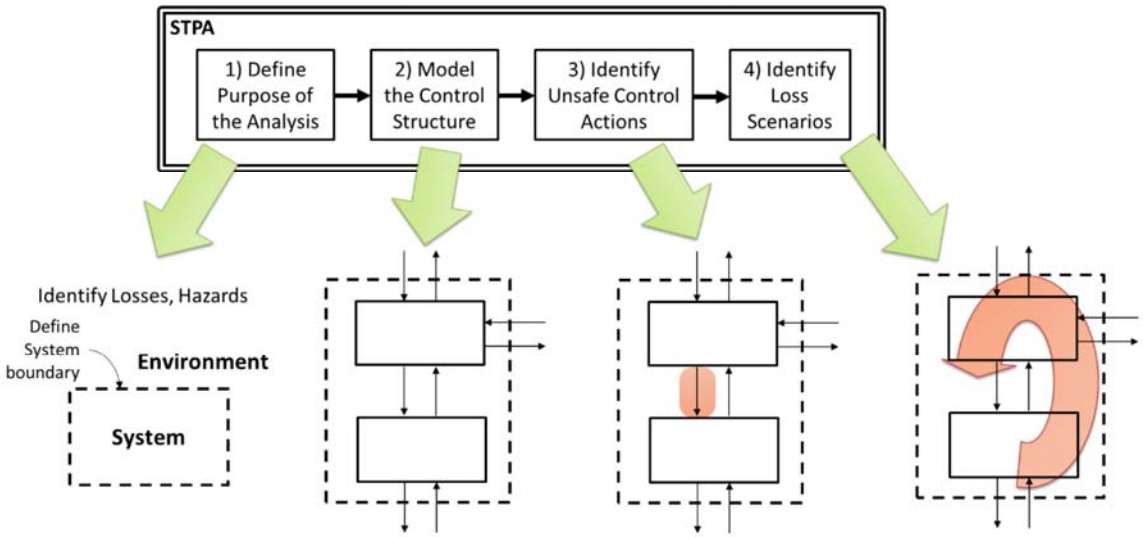

Figure 12. STPA Steps (Leveson & Thomas, 2018)

An overview of STPA steps is presented in Figure 12. STPA techniques are based on abstraction of complex systems. STPA seems to scale well as more details become apparent, and the result is 'scenarios' of what could happen in the event of failure. STPA is used already for NPP operations and is appropriate for the case of microreactors in identifying potential points of concern a priori to full system design and construction.

Integral to performing STPA is a basic understanding of what the control structure of the system will be. Using a basic representation of a system (Figure 13), STPA includes identifying 1) outputs where humans will play a role, and 2) a "map" of the control structure. This control structure informs where additional analysis is appropriate to determine appropriate level of control (or level of automation) at each step and the respective human reliability at these points of operator control.

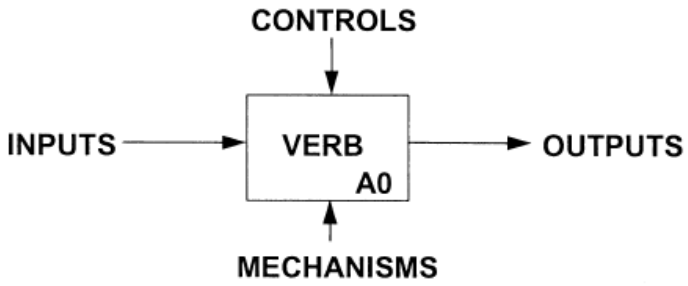

Figure 13. Basic System Representation (Levis & Wagenhals, 2000)

5.3.2. Determine Appropriate Level of Automation

Iteratively conducted with Step 4, Step 5 will determine appropriate types and levels of automation at specific interaction points between the operator and the system. (Parasuraman et al., 2000, 2008) provide guidance for what is appropriate for expected human tasks. (Onnasch, Wickens, Li, & Manzey, 2013) provide another resource to help navigate function allocation for different types of tasks expected of the human operator.

Step 4 helps define the expected states of the entire system and the anticipated points of human intervention or control. The results of this activity inform how much autonomy is desired or required at control points, which defines the role of the human in that context. Guidance from level of automation literature provides a starting point for what is appropriate for expected human tasks.

The output of this activity provides another resource to help navigate function allocation for different types of tasks that require human input. Thus, this step is iterative with the previous step, cycling between the two activities to reconcile potential conflicts and improve fidelity and robustness of the concept.

5.4. Determine Interface Requirements

Finally, Step 6 helps determine how to best support the operator though interface design. Existing standards (see Section 2.3) provide detailed guidance regarding best practices in different control settings. This acts as a starting point for interface/control design.

After reviewing relevant standards, the next activity should focus on apply user-centered design principles and processes to further determine interface and control requirements for safe and reliable operation. This might include concept testing with operators (as a current system does not exist), studying similar designs already deployed (NuScale), and conducting iterative design phases to conceptualize, create, test, and revise features, functions, and capabilities. User testing will help bolster understanding of impacts of potential design changes.

6. CONCLUSIONS

While many of microreactor sites may incorporate autonomous systems, there is no clear definition regarding how automation will be used at the various sites. Further, there's even less understanding of how humans will be involved in on-site and remote decision-making and tasks. A key aspect in the design of microreactors is specifying the level of automation within the system and how much the human will be engaging with that system. For the various levels of automation, there are critical issues that arise that must be explored within the literature. This report is the initiation of a discussion into the factors that influence automation within microreactors.

This report:

- explored the issues around reduced staffing of microreactors;
- highlighted historical safety functions associated with human operators;
- assessed current licensing requirements for appropriateness to varying levels of personnel support; and
- described a recommended regulatory approach for reviewing the impact of reduced staffing to the operation of microreactors.

The NRC has a foundational HFE program outline in NUREG-0711 that establishes a baseline design process for any NPP design. However, implementation of this process may not be sufficient for a system where the operator is located remotely and potentially controlling multiple microreactors from a single operator station. The current NRC framework of applying function allocation and task analysis to identify critical human actions is relevant for microreactor HMI, procedures, and training design. However, since microreactors may have "inherently safe" features, and humans may have limited ability for immediate intervention, designers need to consider all the potential failures that could occur within a microreactor's life. Control mitigations using limited physical human interactions need to be designed into the HMI. Further, analyses should consider the data fidelity of sensors used to provide information about the microreactor's state to the human operator. This fidelity may impact the type of HMI that is able to be incorporated into the microreactor system.

The first two steps within the recommended approach align with the first steps of NUREG-0711. A ConOps is defined for the desired system and indicates the system's goals, assumptions, stakeholder needs, and lifecycle of information. After the ConOps is defined, a designer decomposes the system into a functional architecture, including different aspects of operation. Where the proposed approach slightly diverges is the recommendation to define expected human intervention as the third step in the process. This step does not assign specific roles to personnel, but instead identifies tasks the human would need to perform as well as identify potential hazards a human may need to mitigate. STPA can be used to provide a robust approach to identifying hazards within a given goal structure. Since microreactors may have "inherently safe" features, STPA uses a control structure to identify unsafe control actions. From this model, mechanisms to prevent unsafe modes can be set in place. Iterative with the previous step, the level of automation is defined from the human interventions and iteratively modified as the human intervention is refined. Finally, from the definition of human tasks and level of automation, requirements for an interface can be defined. This phase can also incorporate the specification of procedures and training for using the interface.

6.1. Future Work

Most of the methods presented in this report have been implemented on similar systems in previous research. However, the specification of a functional architecture as it relates to human-system integration for microreactors may be novel for some design types. Additionally, some research has been performed on applying STPA to evaluate the safety of digital instrumentation and control systems in nuclear power plants (Rejzek & Hilbes, 2018; Thomas, de Lemos, & Leveson, 2012). This research could be expanded through an evaluation on the automation of microreactor control systems. The assessment would consider the supervisory role of a human within a SCADA-type system. The output of this analysis could provide insights on safety hazards, safety control structure, identifying unsafe control actions, and translating those actions into safety constraints.

REFERENCES

10 CFR 50: U.S. Code of Federal Regulations, Part 50, Domestic Licensing of Production and Utilization Facilities, Title 10, "Energy."

Adams, S., Cole, K., Haass, M., Warrender, C., Jeffers, R., Burnham, L., & Forsythe, C. (2015). Situation Awareness and Automation in the Electric Grid Control Room. Procedia Manufacturing, 3, 5277-5284. doi:10.1016/j.promfg.2015.07.609

Ahmed, M. M., & Soo, W. L. (2008, 1-3 Dec. 2008). Supervisory Control and Data Acquisition System (SCADA) based customized Remote Terminal Unit (RTU) for distribution automation system. Paper presented at the 2008 IEEE 2nd International Power and Energy Conference.

ANSI/AIAA. (2012). ANSI/AIAA G-043A-2012 In AIAA Guide to the Preparation of Operational Concept Documents. Reston, VA, USA.

Bainbridge, L. (1983). Ironies of automation. Automatica, 19(6), 775-779. doi:https://doi.org/10.1016/0005-1098(83)90046-8

Bedford, T. & Cooke, R. (2001) Mathematical tools for probabilistic risk analysis. Cambridge University Press.

Blanchard, B. S., & Fabrycky, W. J. (2006). Systems engineering and analysis.

Cai, B., Liu, Y., Liu, Z., Wang, F., Tian, X., & Zhang, Y. (2012). Development of an automatic subsea blowout preventer stack control system using PLC based SCADA. ISA Transactions, 51(1), 198-207. doi:https://doi.org/10.1016/j.isatra.2011.08.003

Calhoun, G. L., Ruff, H. A., Behymer, K. J., & Frost, E. M. (2018). Human-autonomy teaming interface design considerations for multi-unmanned vehicle control. Theoretical Issues in Ergonomics Science, 19(3), 321-352. doi:10.1080/1463922X.2017.1315751

Calhoun, G. L., Ruff, H. A., Behymer, K. J., & Mersch, E. M. (2017, 2017//). Operator-Autonomy Teaming Interfaces to Support Multi-Unmanned Vehicle Missions. Paper presented at the Advances in Human Factors in Robots and Unmanned Systems, Cham.

Cheung, S., Dutertre, B., Fong, M. W., Lindqvist, U., Skinner, K., & Valdes, A. (2006). Using Model-based Intrusion Detection for SCADA Networks.

Connors, E., Endsley, M., & Jones, L. (2007). Situation Awareness in the Power Transmission and Distribution Industry. Proceedings of the Human Factors and Ergonomics Society Annual Meeting, 51, 215-219. doi:10.1177/154193120705100415

de Winter, J. C. F., & Dodou, D. (2014). Why the Fitts list has persisted throughout the history of function allocation. Cognition, Technology & Work, 16, 1-11. doi:10.1007/s10111-011-0188-1

Endsley, M. R. (1995). Toward a Theory of Situation Awareness in Dynamic Systems. Human Factors, 37(1), 32-64. doi:10.1518/001872095779049543

Endsley, M. R. (1996). Automation and situation awareness. In Automation and human performance: Theory and applications. (pp. 163-181). Hillsdale, NJ, US: Lawrence Erlbaum Associates, Inc.

Theoretical Underpinnings of Situation Awareness: A Critical Review (Lawrence Erlbaum Associates 2000).

Endsley, M. R. (2016). From Here to Autonomy: Lessons Learned From Human–Automation Research. Human Factors, 59(1), 5-27. doi:10.1177/0018720816681350

Endsley, M. R. (2017). Autonomous Driving Systems: A Preliminary Naturalistic Study of the Tesla Model S. Journal of Cognitive Engineering and Decision Making, 11(3), 225-238. doi:10.1177/1555343417695197

EPRI. (2016). Program on Technology Innovation: Review of Advanced Reactor Technology with Emphasis on Light-Water and Non-Light-Water Small Modular Reactor Designs. EPRI, Palo Alto, CA: 2016. 3002009413.

Ferketic, J., Goldblatt, L., Hodgson, E., Murray, S., Wichowski, R., Bradley, A., . . . Steinfeld, A. (2006). Toward Human-Robot Interface Standards: Use of Standardization and Intelligent Subsystems for Advancing Human-Robotic Competency in Space Exploration. https://doi.org/10.4271/2006-01-2019

Fitts, P. M. (1951). Human engineering for an effective air-navigation and traffic-control system. Washington: National Research Council, Division of Anthropology and Psychology, Committee on Aviation Psychology.

Fleming, E.S. (2013). Developing a Training Program for the Aircraft Collision Avoidance System in context (Master's thesis, Georgia Institute of Technology, Atlanta, GA). Retrieved from https://smartech.gatech.edu/handle/1853/47578

Fleming, E.S., and Pritchett, A.R. (2015) "Training Pilots for Collision Avoidance within a Realistic Operating Context." Journal of Aerospace Systems Information, Vol 12, Special Issue on Aerospace Human-Automation Interaction, pp. 467-475. doi: 10.2514/1.1010291

Flemisch, F., Schwalm, M., Meyer, R., Altendorf, E., Lennartz, T., Schreck, C., . . . Herzberger, N. (2019). Human System Integration at System Limits and System Failure of Cooperatively Interacting Automobiles: Concept and First Results. 52, 93-98. doi:10.1016/j.ifacol.2019.08.054

Fuld, R. B. (1993). The Fiction of Function Allocation. Ergonomics in Design, 1(1), 20-24. doi:10.1177/106480469300100107

Fuld, R. B. (2000). The fiction of function allocation, revisited. International Journal of Human-Computer Studies, 52(2), 217-233. doi:https://doi.org/10.1006/ijhc.1999.0286

Giri, J., Parashar, M., Trehern, J., & Madani, V. (2012). The Situation Room: Control Center Analytics for Enhanced Situational Awareness. IEEE Power and Energy Magazine, 10(5), 24-39. doi:10.1109/MPE.2012.2205316

Greitzer, F. L., Schur, A., Paget, M., & Guttromson, R. T. (2008, 20-24 July 2008). A sensemaking perspective on situation awareness in power grid operations. Paper presented at the 2008 IEEE Power and Energy Society General Meeting - Conversion and Delivery of Electrical Energy in the 21st Century.

Hahn, A., Kregel, B., Govindarasu, M., Fitzpatrick, J., Adnan, R., Sridhar, S., & Higdon, M. (2010). Development of the PowerCyber SCADA security testbed. Oak Ridge, Tennessee, USA: Association for Computing Machinery.

Hicks, T., Warner, M., Miller, G., & Li, J. (SC-29980-201, ML19036A584, December 2018). PRISM Sodium Fast Reactor Licensing Modernization Project Demonstration. Retrieved from

Higgins, J. & Nasta, K. (1996). Human Factors Engineering (HFE) Insights for Advanced Reactors Based Upon Operating Experience (NUREG/CR-6500).

Human Factors and Ergonomics Society. (n.d.). Retrieved March 23, 2020, from https://www.hfes.org/about-hfes/what-is-human-factorsergonomics

IEEE Guide for Information Technology - System Definition - Concept of Operations (ConOps) Document (1362-1998). (1998). IEEE Guide for Information Technology - System Definition - Concept of Operations (ConOps) Document, 1-24.

INCOSE. 2015. Systems Engineering Handbook: A Guide for System Life Cycle Processes and Activities, version 4.0. Hoboken, NJ, USA: John Wiley and Sons, Inc, ISBN: 978-1-118-99940-0

International Atomic Energy Agency. (2018). Integrated Approach to Safety Classification of Mechanical Components for Fusion Applications (IAEA-TECDOC-1851).

International Atomic Energy Agency. (1992). The Role of Automation and Humans in Nuclear Power Plants (IAEA-TECDOC-668).

International Nuclear Safety Advisory Group. (1996). Defence in Depth in Nuclear Safety (INSAG-10).

International Nuclear Safety Advisory Group. (1999). Basic Safety Principles for Nuclear Power Plants (INSAG-12).

Ivergard, Toni, & Hunt, Brian. (2009). Handbook of Control Room Design and Ergonomics: A Perspective for the Future (2nd ed.). Boca Raton, FL: CRC Press.

Joe, J. C., O'Hara, J., Hugo, J. V., & Oxstrand, J. H. (2015). Function Allocation for Humans and Automation in the Context of Team Dynamics. Procedia Manufacturing, 3, 1225-1232. doi:https://doi.org/10.1016/j.promfg.2015.07.204

Kolaczkowski, A., Forester, J., Lois, E., & Cooper, S. (2005). Good practices for implementing Human Reliability Analysis (HRA) (NUREG-1792).

Kossiakoff, A., & Sweet, W. N. (2003). Systems Engineering: Principles and Practice.

Krambeck, D. (2015). An Introduction to SCADA Systems. Retrieved from https://www.allaboutcircuits.com/technical-articles/an-introduction-to-scada-systems/

Leidner, D., Birkenkampf, P., Lii, N., & Borst, C. (2014). Enhancing Supervised Autonomy for Extraterrestrial Applications by Sharing Knowledge between Humans and Robots.

Leveson, N., & Thomas, J. P. (2018). STPA Handbook.

Levis, A. H., & Wagenhals, L. W. (2000). C4ISR architectures: I. Developing a process for C4ISR architecture design. Systems Engineering, 3, 225-247.

Lin, L., & Goodrich, M. A. (2015). Sliding Autonomy for UAV Path-Planning: Adding New Dimensions to Autonomy Management. Istanbul, Turkey: International Foundation for Autonomous Agents and Multiagent Systems.

Macaulay, T., & Singer, B. (2012). Cybersecurity for Industrial Control Systems: SCADA, DCS, PLC, HMI, and SIS. Boca Raton, FL: Taylor & Francies Group, LLC.

Martinie, C., Palanque, P., Navarre, D., & Barboni, E. (2012, 2012//). A Development Process for Usable Large Scale Interactive Critical Systems: Application to Satellite Ground Segments. Paper presented at the Human-Centered Software Engineering, Berlin, Heidelberg.

McGrew, R. W., & Vaughn, R. B. (2009). Discovering vulnerabilities in control system human–machine interface software. Journal of Systems and Software, 82(4), 583-589. doi:https://doi.org/10.1016/j.jss.2008.12.049

Mitchell, C. M. (1987). GT-MSOCC: A Domain for Research on Human - Computer Interaction and Decision Aiding in Supervisory Control Systems. IEEE Transactions on Systems, Man, and Cybernetics, 17(4), 553-572. doi:10.1109/TSMC.1987.289347

MITRE. (n.d.). Concept of Operations.

Morsi, I., Deeb, M. E., & Zwawi, A. E. (2009, 15-20 Nov. 2009). SCADA/HMI Development for a Multi Stage Desalination Plant. Paper presented at the 2009 Computation World: Future Computing, Service Computation, Cognitive, Adaptive, Content, Patterns.

Naderpour, M., Lu, J., & Zhang, G. (2014). An intelligent situation awareness support system for safety-critical environments. Decision Support Systems, 59, 325-340. doi:https://doi.org/10.1016/j.dss.2014.01.004

NRC. (1982). Guidelines for the preparation of emergency operating procedures (NUREG-0899).

NRC. (1993). Training review criteria and procedures (NUREG-1220).

NRC. (1998). Knowledge & abilities catalogue for NPP operators: PWRs (NUREG-1122).

NRC. (2005). Guidance for Assessing Exemption Requests from the Nuclear Power Plant Licensed Operator Staffing Requirements Specified in 10 CFR 50.5m (NUREG-1791)

NRC. (2007). Knowledge & abilities catalogue for NPP operators: BWRs (NUREG-1123).

NRC. (2011). Nuclear power plant simulators for use in operator training (Regulatory Guidance 1.149, Rev 4).

NRC.(2016). Standard Review Plan: Chapter 18 - Human Factors Engineering (NUREG-0800).

Nuclear Energy Institute. (2016). Diverse and Flexible Coping Strategies (FLEX) Implementation Guide (NEI 12-06 Rev 4).

NuScale Power (2019). Concept of Operations (RP-0215-10815-NP).

O'Hara, J., Brown, W., Lewis, P., & Persensky, J. (2002). Human-System Interface Design Review Guidelines (NUREG-0700).

O'Hara, J., Higgins, J., Fleger, S., & Pieringer, P. (2012). Human Factors Engineering Program Review Model (NUREG-0711)

Onnasch, L., Wickens, C. D., Li, H., & Manzey, D. (2013). Human Performance Consequences of Stages and Levels of Automation: An Integrated Meta-Analysis. Human Factors, 56(3), 476-488. doi:10.1177/0018720813501549

Panteli, M., & Kirschen, D. S. (2015). Situation awareness in power systems: Theory, challenges and applications. Electric Power Systems Research, 122, 140-151. doi:https://doi.org/10.1016/j.epsr.2015.01.008

A model for types and levels of human interaction with automation, 30 286-297 (2000).

Parasuraman, R., Sheridan, T. B., & Wickens, C. D. (2008). Situation Awareness, Mental Workload, and Trust in Automation: Viable, Empirically Supported Cognitive Engineering Constructs. Journal of Cognitive Engineering and Decision Making, 2(2), 140-160. doi:10.1518/155534308X284417

Price, H. E. (1985). The Allocation of Functions in Systems. Human Factors, 27, 33-45. doi:10.1177/001872088502700104

Price, H., Maisano, R., & Van Cott, H. (1982). Allocation of functions in man-machine systems: a perspective and literature review (NUREG/CR-2623). United States

Prostejovsky, A. M., Brosinsky, C., Heussen, K., Westermann, D., Kreusel, J., & Marinelli, M. (2019). The Future Role of Human Operators in Highly Automated Electric Power Systems. Electric Power Systems Research, 175,[105883]. https://doi.org/10.1016/j.epsr.2019.105883

Pulliam, R., Price, H., Bongarra, J., Sawyer, C., & Kisner, A. (1983) Methodology for allocating nuclear power plant control functions to human or automatic control. United States.

Rasmussen, Jens. (1983). Skills, Rules, and Knowledge; Signals, Signs, and Symbols, and other Distinctions in Human Performance Models. IEEE Transactions on Systems, Man and Cybernetics, 13(3), 257-266.

Rasmussen, Jens, & Vicente, Kim. (1989). Coping with human errors through system design: implications for ecological interface design. International Journal of Man-Machine Studies, 31, 517-534.

Reason, J. (1990). Human Error. Cambridge University Press.

Rejzek, M., & Hilbes, C. (2018) Use of STPA as a diverse analysis method for optimization and design verification of digital instrumentation and control systems in nuclear power plants. Nuclear Engineering and Design, 331, 125-135.

Russell, R. I., & Golden, C. (1996). Human computer interface (HCI) standards for cost effective satellite control. In Space Programs and Technologies Conference: American Institute of Aeronautics and Astronautics.

Sayed, K., & Gabbar, H. A. (2017). SCADA and smart energy grid control automation. In (pp. 481-514).

Sheridan, T. B. (1992). Telerobotics, Automation, and Human Supervisory Control.

Sheridan, T. B. (2000). Function allocation: algorithm, alchemy or apostasy? International Journal of Human-Computer Studies, 52, 203-216. doi:10.1006/ijhc.1999.0285

Sheridan, T.B. (2012). Human Supervisory Control 990-1015 (John Wiley & Sons, Inc. 2012). 4th.

Sheridan, T. B. (2016). Human – Robot Interaction: Status and Challenges. Human Factors, 58, 525-532. doi:10.1177/0018720816644364

Sheridan, T. B., & Ferrell, W. R. (1974). Man-machine systems; Information, control, and decision models of human performance. Man-machine systems; Information, control, and decision models of human performance., ix, 452-ix, 452.

Sowder, A. & Marciulescu, C. (2016) Program on Technology Innovation: Review of Advanced Reactor Technology with Emphasis on Light-Water and Non-Light-water Small Modular Reactor Designs (EPRI 3002009413)

Tenhundfeld, N. L., de Visser, E. J., Haring, K. S., Ries, A. J., Finomore, V. S., & Tossell, C. C. (2019). Calibrating Trust in Automation Through Familiarity With the Autoparking Feature of a Tesla Model X. Journal of Cognitive Engineering and Decision Making, 13(4), 279-294. doi:10.1177/1555343419869083

Thieme, C. A., & Utne, I. B. (2017). A risk model for autonomous marine systems and operation focusing on human–autonomy collaboration. Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability, 231(4), 446-464. doi:10.1177/1748006X17709377

Thomas, J. de Lemos, F., & Leveson, N. (2012) Evaluating the Safety of Digital Instrumentation and Control Systems in Nuclear Power Plants. NRC-HQ-11-6-04-0060.

Timbus, A., & Bitto, M. (2015). Symphony Orchestrates. ABB Review, 15(4).

Wilson, J. (2004). Design Certification Process. In 4rd NRC – AERB Nuclear Safety Projects Meeting: United States Nuclear Regulatory Commission.

Wood, B. (2019, August 29, 2019). Advanced SCADA functionality helps solar operators manage the future. Solar Power World, August. Retrieved from https://www.solarpowerworldonline.com/2019/08/advanced-scada-functionality-solar-trimark/

Wright, P., Dearden, A., & Fields, B. (1999). Function allocation: A perspective from studies of work practice. International Journal of Human-Computer Studies, 52, 335-355. doi:10.1006/ijhc.1999.0292

Zolotová, I., & Landryová, L. (2005). Knowledge model integrated in SCADA/HMI system for failure process prediction. Prague, Czech Republic: World Scientific and Engineering Academy and Society (WSEAS).

APPENDIX A. SME INTERVIEW QUESTIONS

A.1. Interview Protocol: Microreactor Researchers

1. Name:
2. Years of Experience with microreactor research (or Advanced Reactor research):
3. What experiences have you had with microreactors?
4. Within your role, how are you planning on using microreactors?
5. What do you envision is the human involvement in running the reactor on a day-to-day basis?
6. What do you envision is the human's role in maintenance operations?
7. What contingencies, emergencies, and non-nominals might occur within operation of the plant (not just the reactor)? (e.g. weather events, adversary intervention, cooling system issues)
8. How might the human intervene in these situations?
9. What literature/authors should be included within a literature search related to the automation of microreactors?
10. Is there anyone else you think we should talk with?

A.2. Interview Protocol: NRC Policies

1. Name:
2. Years of Experience with Nuclear Reactors:
3. What is your background related to Nuclear Reactors?
4. What experiences have you had with microreactors?
5. What is the role of the human in current reactor operations? (i.e. reactors that are currently approved and licensed for use by the NRC)
6. What contingencies, emergencies, and non-nominals might occur within operation of the plant (not just the reactor)? (e.g. weather events, adversary intervention, cooling system issues)
7. How does the human currently intervene in these situations? How might a human be required to intervene in future scenarios? I.e. could automation take the place of a human's role in emergency situations?
8. What would it take for you to certify a fully autonomous microreactor? What current regulations would stand in the way of automating microreactors?
9. Is anyone at NRC (or a partner of NRC) working on issues related to the introduction, certification, or licensing of microreactors?
10. What literature/authors should be included within a literature search related to the automation of microreactors?
11. Is there anyone else you think we should talk with?

APPENDIX B. SME INTERVIEW NOTES

B.1. NRC SME Interview Notes

Interview Protocol: NRC Policies

1. Name:

- [Redacted A]
- [Redacted B]
- [Redacted C]

2. Years of Experience with Nuclear Reactors (N/A)

3. What is your background related to Nuclear Reactors? (N/A)

4. What experiences have you had with microreactors?

Core Review team- includes HF staff. Been engaged with pre-application reviews for a couple different designs/discussions.

Outside the scope of this, wrapping up reviews for the NuScale small modular reactor design. LWR. Fairly early stages of microreactor discussions. In meetings about the general approaches that applicants are considering for designs. Looking at what needs to be in place to formally conduct reviews.

Part of what they're hearing in these discussions are issues that were raised in LTD6. Possibility of autonomous operations. Remote operations. Highly automated or fully passive designs. Given nature of the review process, the NRC historically uses HF guidance for large LWR. These facilities pose substantially greater risk to the public than the new designs. Relied much more heavily on operator action to mitigate accidents.

Been looking at this from HF perspective for a new review approach that would be more appropriately suited to the level of risk, nature of the operations, nature of the orgs coming in, right size and right focus to address these types of applications.

SNL Q: have they had any actual applications?

A: Pre-Application discussion.

5. What is the role of the human in current reactor operations? (i.e. reactors that are currently approved and licensed for use by the NRC)

Staffing requirements: NRC regulations require operating experience for a specific number of years, units, configurations. Regulations are based on large reactors. But, new designs don't fit existing staffing requirements. For NuScale, had to prove out through validation exercises that they could operate the facility through fewer staff.

The requirements would not be practical for microreactors because they would be prohibitive for microreactor output. Wouldn't be deemed to be necessary based on the simplicity of design.

SNL Q: Would the requirements have to be changed? A: The NuScale applicant was able to proceed based on a licensing pathway that didn't require a change. But, ultimately it would make sense for the agency to not require prescriptive staffing requirement.

6. What contingencies, emergencies, and non-nominals might occur within operation of the plant (not just the reactor)? (e.g. weather events, adversary intervention, cooling system issues)
Challenge- Applications may vary across different vendors. One answer may not be sufficient for all. It's natural based on our history to say "of course," because of what a large LWR would require.
[For the large reactors] There would have to be many situations that would require the operator there. I think until we have more information, it's going the be hard to know if claims are true.

7. How does the human currently intervene in these situations? How might a human be required to intervene in future scenarios? I.e. could automation take the place of a human's role in emergency situations?
[For microreactors] Little required by human operator. Passive designs as design matures, but there's a recognition that operator actions are required for certain activities. Might have a control station to monitor multiple stations (remote monitoring station)

SNL Q: What types of events might the human be involved in?
A: something they're trying to explore. Largely a monitoring function. Design of reactor physics should be to naturally shut down the reactor if there is at risk conditions. Reactor may naturally go to a safe state. Start-up sequence. Control, power management functions- to adjust reactor output on demand.

8. What would it take for you to certify a fully autonomous microreactor? What current regulations would stand in the way of automating microreactors?
For remote: Understand the risk to the public (size of core, worst case scenario for reactor to fail). That will be the beginning. If the answer is the worst thing that could happen is some minimal dose within the controlled boundary of this facility triggers occupational exposure but not detrimental to health and safety then you can say
For autonomous: whether we're looking at a facility in which the physics of the reactor make it so that it can be autonomous and shut down as needed (passive). Or, are active components dependent on complex control logic? More concerns about how confident we can be that active components controlled by computer logic are effective without human backstop.
Bar for consequences of failure is much lower than large LWR. Expected to be risk-informed in approach.
Will have to certify software. Physics is not as concerning as external software or mechanical functions.

9. Is anyone at NRC (or a partner of NRC) working on issues related to the introduction, certification, or licensing of microreactors?
NuScale certification: NUREG on staffing exemption process. Provided the broad framework for how they were able to proceed with NuScale. But, would need to check with the people who did that review. Needed to include a design specific staffing requirement for the NuScale design. Rather than taking an exemption.

10. What literature/authors should be included within a literature search related to the automation of microreactors?

11. Is there anyone else you think we should talk with?

Other Comments:
Role of the operator and performance of the operator- used generally because some of these things we can regular but when we think of from a safety perspective. Coming at from a broad human performance perspective. How it would affect the number of people on site.
Licensing and changes to the licensing process.
Risk to the plant and non-plant personnel (other hazards, combustibles,)
To what extent are we using proven technologies vs novel technologies
Consideration to the site of the plant (how remote)- has implications for emergency preparedness, also impacts personnel placement (sociological influences)
Remote operation of the facility (individuals aren't at plant. Where are they located?)
Frequency and extent of NRC oversite—in the past had resident inspectors, etc. Would that change?
Plant operating characteristics
Relying on passive or active features to control
Surveillance vs monitoring remote sensors (limited operating experience may lead to degraded performance)
Plant emissions

B.2. LANL SME Interview Notes

Interview Protocol: Microreactor Researchers

1. Name: [Redacted]

2. Years of Experience with microreactor research (or Advanced Reactor research): (N/A)

3. What experiences have you had with microreactors?
Used to run Melcore. Part of Level 1, 2, and 3 risk. Within DOE Nuclear Energy (NE)- Idaho, Argonne, Oakridge that support nuclear power business (Commercial reactor industry). After 2006, LANL kicked out of commercial reactor industry.
(1) Looked at the army reactor program ('60s) – 1kW to 1mW. Design small power heatpipe based reactors for military bases, fits on semitruck. Portable DOD reactor.
Westinghouse has licensed some aspects of their designs, but mostly just kept heatpipe mechanism. Working with Westinghouse but not making design decisions. Most of the work is inhouse for Westinghouse.
(2) Space reactors – DUFF (Demonstration Using Flattop Fissions) and KRUSTY. Focused on <10mW reactors on physics side (not on power conversion).

4. Within your role, how are you planning on using microreactors?
[See Q3]
Both defense and space usage. National security lab- so more government applications.

5. What do you envision is the human involvement in running the reactor on a day-to-day basis?
Because of size of microreactors, the power density is low. When you have megawatts of heat to remove, that can cause problems… as you reduce the size of the nuclear reactor, these problems are significantly reduced.
You can make a microreactor self-regulating. Make the reactor dependent on the power conversion (tightly coupled). E.g. space reactor has to be automated because no people. Get reactors that would respond through physics.
Have planned for people to remotely monitor (set the output and maybe turn on and off).
Physics- designed to make reactor want to be at a specific temperature. But, if the power conversion wants more power, the temperature drops. Reactor contracts a little due to temp drop. Sheds less neutrons. Opposite true for less power. Thus, reactor adjusts itself.
Maximize self-regulation. But, not maximizing uranium usage (ie power ain't cheap).
Single stepper motor that pulls rod in and out. (rods adjust temperature) For space reactor, no redundancy.

In most small reactors, won't see a steam rankin cycle. Very small ranges- sterling engines. Next: gas braten system (Not changing phase. Just taking a hot gas and putting it through. Loose efficiency but vastly smaller)…. One version you use gas and eject. Other version you reuse.

Human- start stop option and maybe human wouldn't need to change the temperature equilibrium point. Microreactor doesn't need a lot of human interaction. Just there to produce power. Can ramp up or down on power conversion. Could pair with other energy sources (e.g. solar). Human would only interact with some type of dial to adjust the power output.

6. What do you envision is the human's role in maintenance operations?
In space- no one has the ability to fix anything or maintain anything. For the DOD didn't want that either. Would just have a set lifetime. If something broke, then it's broken. It would be shut down and sent home.

7. What contingencies, emergencies, and non-nominals might occur within operation of the plant (not just the reactor)? (e.g. weather events, adversary intervention, cooling system issues)
How might the human intervene in these situations?
Safety consideration- e.g. radiation release- dependent on size of the microreactor. E.g. level 1 risk
What's probability of melting fuel? In Level 1 PRA look for human factors or ways things fail that lead to core melt. How could we decay reactor and not be able to get rid of heat?
For Kilopower project- showed they could turn off all active cooling. Didn't scram reactor but it still dropped in temperature and it was still "happy as a clam" based on physics of heat leak. PM says he doesn't know if it can meltdown.
If it were working correctly- would just check periodically on temperature balance and other metrics.
Envision a need to Scram? Space no. Terrestrial yes. E.g. if power system fails. Need to send power system back to factor. Hear a noise, power's shot. Reactor's shot. Not making power no use in the reactor. Call guys "lost the turbine" they say "wait 7 days then we'll send it back"
OR if they lost a base then might need to scram to send the reactor back.
What about security- what could a bad agent do? Could they make it dirty? A terrorist could blow it up and spread fission products.
Could they steal the materials? Anything terrestrial would be LEU <20% enriched. For space would be HEU.

8. What literature/authors should be included within a literature search related to the automation of microreactors?
Kilopower & Megapower documents. Could send us some documents.

9. Is there anyone else you think we should talk with?
[Sandia Braten Lab, Sandia Super critical CO2]
Can get us names of people at Westinghouse. DD Rao.
Oklo. Bwxt. X Energy.

B.3. EPRI SME Interview Notes

Interview Protocol: Microreactor Researchers

1. Name: [Redacted]

2. Years of Experience with microreactor research (or Advanced Reactor research):
20 years experience

3. What experiences have you had with microreactors?
- Operational experience with Navy
- Training facility, prototype and on aircraft carriers
- At Jensen Hughes (before it was JH). Has worked on risk assessment.
- Academic, university. Science
- Now, more research-based with national labs
- AT EPRI:
    - Has spoken to staff at Westinghouse and Oklo and National Labs about microreactors
    - Does own research looking at microreactors
- Has had interactions with small reactors (maintenance) + panels (preventative maintenance, corrective maintenance) throughout career

4. Within your role, how are you planning on using microreactors?
- What are the applications of microreactors? Applications of microreactors is pretty wide (DOD, commercial, off-grid, etc)
- High-barrier to entry (staffing, etc) all applies to modern larger reactors
    - If they say no emergency planning zone (EPZ) required, what does that mean?
    - For the forseeable future, [the microreactor is] on it's own site.
    - Site boundary could be small (acres) but not a city block

5. What do you envision is the human involvement in running the reactor on a day-to-day basis?
- For autonomous- no humans. Technology monitoring, so it would bring back into balance if needed.
- Wording is very critical- very important how you communicate these technologies.
- Human interactions at the monitoring level is redundant. Humans now are already "remote," and separated by shielding.
    - Issues with cyber security and the growth of adversary technology
- Fundamental design of the device—how complex did you make this thing?
    - If accident tolerant fuel, then ok…. risk assessment is very important
- Capitulated from a regulatory standpoint to provide more engineering and rigidity to provide safety
    - As the latest greatest developments have come, it's tough to meet yesterday's requirements
    - Requirements are too prescriptive
- When systems are more simplified, they'll have less operating systems and less parameters (lots of N/A for the requirements)
    - Related to latest and greatest licensing projects
    - CFR Part 50, Part 52 -- regulations

6. What do you envision is the human's role in maintenance operations?

- Design-specific
  - Turbine- then specific to maintaining those, Etc
- Every 12 years- fuel shuffling
- Sensors that will break? Maybe

7. What contingencies, emergencies, and non-nominals might occur within operation of the plant (not just the reactor)? (e.g. weather events, adversary intervention, cooling system issues)
How might the human intervene in these situations?

- Cyber
- Evacuation
- Site-dependent: where is the device? Ease of physical access
  - e.g. reactors on military bases
- Depends on the design
  - Backup ac?
  - Diesel generator required?
  - Multiple microreactors?
  - Could build something that's fairly hardened with redundancy. Redundant fuel cell and hydrogen on site.
  - Decrease the threat vectors through redundancy
- Things operating at low pressure vs high pressure, gets rid of some risk
- Threats
  - Inside actors
  - Cyber
  - Physical security

8. What literature/authors should be included within a literature search related to the automation of microreactors?

- Advanced nuclear technology (ANT) economic-based research and development roadmap for nuclear powerplant construction (EPRI 3002015935)
- Economics Roadmap on Reactor Deployment
- Titans of nuclear podcast (NEI, EPRI,)

9. Is there anyone else you think we should talk with?

- Operating characteristics
- Licensing pathways
- Licensing support
- Deployments
- <ppl who build reactors>
- Titans of nuclear: podcast. Bret Kugelmass
- Yasar Arafat (Westinghouse – now INL)
- Sen Lisa Murkowski
- Senate committee of energy and natural resources
- Pandora's promise (2013 documentary)
- New Fire (Documentary)

    - David Schumaker
    - The executive producer

10. Near-term
- Licensing and Modernization Project (NRC): INL
- Existing pipelines and channels don't support the proposed path forward
- Wrap-up existing work on modernizing other plants. Identify existing entities and stakeholders
- Community of existing stakeholders that are submitting their designs for regulatory reviews
    - E.g. microreactor that needs existing work
    - Design is still very conceptual, not all analyses have been conducted
    - Building into a design certification document (DCD)
    - DCD- has prescribed table of contents
- Expectation of a regulator or a licensing agent has documentation already existing…. Design maturity
- Under research reactors there is a licensing protocol that exists that the microreactors can go through (license starts with R)
- Sufficient –
    - Unsure if they're sufficient processes
- Documents are very prescriptive
    - Too the level of degrees people have to have to operate the reactor

11. What would it take for you to certify a fully autonomous microreactor? What current regulations would stand in the way of automating microreactors?
- NUREGs—
- Etc. evacuating
- Even how we communicate to the public evacuations is from 1980 (old tech.. broad but still out of date)

DISTRIBUTION

Email—External

Name	Company Email Address	Company Name
Joseph Sebrosky	Joseph.Sebrosky@nrc.gov	NRC
William Reckley	William.Reckley@nrc.gov	NRC
Lucieann Vechioli	Lucieann.VechioliFeliciano@nrc.gov	NRC

Email—Internal

Name	Org.	Sandia Email Address
David L. Luxat	8852	dlluxat@sandia.gov
Elizabeth Fleming	6671	eflemin@sandia.gov
Jason Morris	6671	jmorris@sandia.gov
Megan Nyre-Yu	6671	mnyreyu@sandia.gov
Paul Schutte	6671	pschutt@sandia.gov
Scott E. Sanborn	8854	sesanbo@sandia.gov
Caren Wenner	6670	cawenne@sandia.gov
Technical Library	9536	libref@sandia.gov

This page left blank

This page left blank

Sandia National Laboratories

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia LLC, a wholly owned subsidiary of Honeywell International Inc. for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.