BROOKHAVEN
NATIONAL LABORATORY

BNL-96881-2012

Human Reliability Considerations for Small Modular Reactors

John O’Hara and Jim Higgins
Brookhaven National Laboratory
Nuclear Science and Technology Department
Systems Engineering Group
Upton, NY 11973

Amy D’Agostino and Erasmia Lois
Division of Risk Analysis
Office of Nuclear Regulatory Research
U.S. Nuclear Regulatory Commission
Washington, DC 20555

January 27, 2012

Nuclear Science and Technology Department
Systems Engineering Group

Brookhaven National Laboratory

U.S. Department of Energy

DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, nor any of their contractors, subcontractors, or their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or any third party's use or the results of such use of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof or its contractors or subcontractors. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof..

Project: Human Factors Aspects in CONOPS of Modular Design (NRC JCN N-6862)
Deliverable: Task 4 Technical Letter Report
BNL Technical Report No. BNL-96881-2012

Human Reliability Considerations for Small Modular Reactors

Prepared for:

Division of Risk Analysis
Office of Nuclear Regulatory Research
U.S. Nuclear Regulatory Commission
Washington, DC 20555

Prepared by:

John O'Hara and Jim Higgins
Brookhaven National Laboratory
Nuclear Science and Technology Department
Systems Engineering Group
Upton, NY 11973

Amy D'Agostino and Erasmia Lois
Division of Risk Analysis
Office of Nuclear Regulatory Research
U.S. Nuclear Regulatory Commission
Washington, DC 20555

January 27, 2012

Abstract

Small modular reactors (SMRs) are a promising approach to meeting future energy needs. Although the electrical output of an individual SMR is relatively small compared to that of typical commercial nuclear plants, they can be grouped to produce as much energy as a utility demands. Furthermore, SMRs can be used for other purposes, such as producing hydrogen and generating process heat. The design characteristics of many SMRs differ from those of current conventional plants and may require a distinct concept of operations. The U.S. Nuclear Regulatory Commission (NRC) conducted research to examine the human factors engineering and the operational aspects of SMRs. The research identified thirty potential human-performance issues that should be considered in the NRC's reviews of SMR designs and in future research activities. The purpose of this report is to illustrate how the issues can support SMR probabilistic risk analyses and their review by identifying potential human failure events for a subset of the issues. As part of addressing the human contribution to plant risk, human reliability analysis practitioners identify and quantify the human failure events that can negatively impact normal or emergency plant operations. The results illustrated here can be generalized to identify additional human failure events for the issues discussed and can be applied to those issues not discussed in this report.

Table of Contents

List of Figures

List of Tables

1 Introduction

The purpose of this report is to identify how the results of our research on the human-performance issues associated with small modular reactors (SMRs) can be applied to support risk analyses of them.

SMRs are a promising approach to meeting future energy needs. Although the electrical output of an individual SMR is relatively small compared to that of typical commercial nuclear plants, they can be grouped to produce as much energy as a utility demands. Furthermore, SMRs can be used for other purposes, such as producing hydrogen and generating process heat. The design characteristics of many SMRs differ from those of current conventional plants and may require a distinct concept of operations (ConOps). In this U.S. Nuclear Regulatory Commission (NRC) conducted a research project to examine the human factors engineering (HFE) and the operational aspects of SMRs (O'Hara, Higgins & Pena, 2012). We identified potential issues in human performance related to the design and operations of SMRs. For our purposes, the term "issue" refers to:

- an aspect of SMR development or design for which information connotes a negative impact on human performance

- a feature of SMR development or design that might degrade human performance, but where additional research and/or analysis is needed to better understand and quantify that impact

- a technology or technique that will be used in designing new plants or implementing them for which there is little or no review guidance

We identified 30 such issues; listed in Table 1-1. Two of the issues are directly related to probabilistic risk assessment (PRA): (1) PRA Evaluation of Site-wide Risk, and (2) Identification of Risk-important Human Actions when One Operator/Crew is Managing Multiple SMRs.

NRC licensees and applicants perform PRAs to assess the risk associated with nuclear power plants (NPPs) and to develop an understanding of plant capabilities and weaknesses contributing to the risk. PRA results are used to identify improvements needed to reduce risk. A brief summary of the two issues is provided below.

The first issue is "PRA Evaluation of Site-wide Risk." Current PRAs in the United States address two- or three-unit sites. However, SMR sites may have many more units. Therefore, modeling SMRs, especially those with shared systems, probably will require new models for PRAs. A single-unit PRA considers common- or site-wide systems such as offsite power, AC power on site, the ultimate heat sink, and various cross-connections between units, such as air- and cooling-water systems. They also cover the effect on individual units of site-wide initiating events, such as loss of offsite power, station blackout, seismic events, and external floods. PRAs may need upgrading to encompass site-wide risk for multiple units. A site-wide PRA may evaluate potential core damage (CD) at multiple units caused by site-wide initiating events and the influences of common systems and a common control room as potential common-cause failures. This site-wide PRA may result in CD at multiple units, but at a lower frequency than for a single unit. However, the PRA level 2 releases could be potentially higher due to CD at multiple units. This is a PRA-related policy issue that should be addressed by the NRC staff and possibly industry groups such as the Nuclear Energy Institute or the American Nuclear Society.

Table 1-1 Potential Human-Performance Issues[1]

ConOps Dimension	Human Performance Issue
Plant Mission	**New Missions**
	Novel Designs and Limited Operating Experience from Predecessor Systems
Agents' Roles and Responsibilities	**Multi-unit Operations and Teamwork**
	High Levels of Automation for All Operations and Its Implementation
	Function Allocation Methodology to Support Automation Decisions
Staffing, Qualifications, and Training	New Staffing Positions
	Staffing Models
	Staffing Levels
Management of Normal Operations	Different Unit States of Operation
	Unit Design Differences
	Operational Impact of Control Systems for Shared Aspects of SMRs
	Impact of Adding New Units While Other Units are Operating
	Managing Non-LWR Processes and Reactivity Effects
	Load-following Operations
	Novel Refueling Methods
	Control Room Configuration and Workstation Design for Multi-Unit Teams
	HSI Design for Multi-unit Monitoring and Control
	HSIs for New Missions (e.g., steam production, hydrogen)
Management of Off-normal Conditions and Emergencies	Safety Function Monitoring
	Potential Impacts of Unplanned Shutdowns or Degraded Conditions of One Unit on Other Units
	Handling Off-Normal Conditions at Multiple Units
	Design of Emergency Operating Procedures (EOPs) for Multi-Unit Disturbances
	New Hazards
	Passive Safety Systems
	Loss of HSIs and Control Room
	PRA Evaluation of Site-wide Risk (i.e., across all units)
	Identification of Risk-Important Human Actions (RIHAs) when One Operator/Crew is Managing Multiple SMRs
Management of Maintenance and Modifications	Modular Construction and Component Replacement
	New Maintenance Operations
	Managing Novel Maintenance Hazards

1. The bold items are discussed in Section 3 of this report.

The second issue is "Identification of Risk-important Human Actions when One Operator/Crew is Managing Multiple SMRs." An area where new techniques may be needed is the identification of risk-important human actions (RIHAs). Plant designers typically identify and address them in their HFE programs. If the PRA is more difficult to model, it will be harder accurately to identify RIHAs. Even when the units themselves are deemed independent; i.e., no shared systems and the units are separated physically, there is the potential for human error if the same operator/crew monitors them. For example, the potential for human error for one unit may increase if the operator's attention is directed to another unit. Modifications may be needed to PRA methods to account for these effects.

While research is needed to address the two specific SMR-related PRA issues discussed above, the purpose of this report was to identify how the results of our research on SMR human-performance issues can be applied to the PRAs for SMRs. Many of the SMR human performance issues can be used by PRA practitioners in the development of a plant-specific human reliability analysis (HRA). HRA is the portion of PRA that models and evaluates the human contribution to risk. HRA practitioners identify and quantify the human failure events that can negatively impact normal or emergency plant operations. HRA is "a structured approach used to identify potential human failure events and to systematically estimate the probability of those events using data, models, or expert judgment" (ASME/ANS, 2009).

Thus to identify how our results can be used by PRA/HRA practitioners, we identified potential human failure events for a subset of the issues (bolded in Table 1-1). The human failure events we have identified are based on the descriptions of the SMR human-performance challenges discussed in each issue. The human failure events are stated in generic terms; unlike the actual human failure events developed by HRA practitioners during PRA modeling for a specific plant design.

The results illustrated here can be generalized to identify additional human failure events for the issues discussed and can be applied to those issues not discussed in this report.

The remainder of this report discusses HRA technology at a high level in Section 2, providing references to guidance documents for performing HRA as well as guidance for selecting and applying the appropriate HRA method. Section 3 presents the human failure events for selected SMR human-performance issues. Conclusions are discussed in Section 4.

2 Current HRA Technology

HRA is the portion of PRA that models and evaluates the human contribution to risk. HRA identifies and quantifies the human failure events that can negatively impact normal or emergency plant operations. Human failure events are modeled in the PRA (event trees and fault trees) and represent function, system, or component failures resulting from one or more unsafe actions. Unsafe actions are actions inappropriately taken by personnel, or not taken when needed, that result in degraded plant safety (Forester et al., 2007).

Human failure events associated with normal plant operation, called pre-initiators, include human actions that leave the plant in an unrevealed and unavailable state. For example, a valve may be misaligned during normal operations; thus, when it is unavailable when needed in subsequent upset conditions. Human failure events associated with emergency plant operations, called post-initiators, include human actions that inhibit the system from performing its function. Post initiators occur as part of the response of personnel to an upset condition. For example, a crew may open a valve that should not be open, leaving the system unable to perform its intended function. Quantification of the probabilities of these human failure events is based on plant and accident specific conditions, including any dependencies among the human actions (i.e., probability of success/failure on one action changes the probability of success/failure on a subsequent action).

HRA is comprised of three major tasks:

- Identification of human failure events (pre or post initiator) that would result in an initiating event or may impact the mitigation of an initiating event.

- Qualitative analysis comprised of:

    - Systematic examination of the *conditions* under which the human actions modeled in the PRA must be performed

    - Systematic examination of the *operational features* that influence the crew's ability to accomplish required tasks (e.g., HSI, procedure availability/quality, crew size, training and expertise).

- Quantitative analysis comprised of estimation of human error probabilities based upon the conditions and features identified in the qualitative analysis.

Given the continuing importance of PRAs in regulatory decision-making, it is crucial that decision-makers have confidence in the PRA results, including associated HRAs. Consequently, the NRC has undertaken initiatives to ensure the quality of both PRA and HRA:

- *An Approach for Determining the Technical Adequacy of Probabilistic Risk Assessment Results for Risk-Informed Activities* (Regulatory Guide 1.200; NRC, 2009) provides an approach for determining the technical adequacy of PRA results for risk-informed regulatory decision-making.

- *Good Practices for Implementing Human Reliability Analysis* (NUREG-1792; Kolaczkowsi et al., 2005), and *Evaluation of HRA Methods Against the Good Practices* (NUREG-1842; Forest et al., 2006) evaluate various HRA methods commonly used in regulatory applications based on their capabilities to satisfy the good practices.

These documents are noteworthy because they help HRA practitioners choose from the many HRA methods that are currently available. NUREG-1842 specifically focuses on HRA methods that use one of three general quantification approaches:

- Adjusts basic HEPs or otherwise determines the HEPs according to a list of influencing factors specifically addressed by the method.

- Uses a more flexible context-defined set of factors and expert judgment to estimate the final HEP.

- Uses (to the extent practical) empirical information based on simulations of accident scenarios in power plant simulators.

All of these approaches have associated strengths and limitations that should be understood to ensure thoughtful application of a method. For example, empirically based quantification can provide a level of credibility in the results that may be considered superior to expert judgment techniques. However, as a limitation, it is not practical to obtain empirical evidence about every human action that may be of interest for all types of sequences. This necessitates using limited empirical evidence for situations and sequences that were not simulated, potentially questioning the suitability of applying the information to these other situations; hence, the need for thoughtful use of the limited data and appropriate justification of its applicability wherever used.

NUREG-1842 concluded that no one approach is always better than another as long as good HRA practices are followed (Forest et al., 2006). The suitability of a method will depend on the application and the potential tradeoffs involved (e.g., how close the empirical evidence fits the situation being assessed, or whether a method's list of treated influences captures those most relevant to the action being addressed). The NRC staff developed a framework in NUREG-1842, to guide the selection of an existing method for a given application.

Given the numerous HRA methods available, Figure 2-1 provides a framework for analysts to select an HRA method appropriate to their application, and for reviewers to confirm that the HRA method chosen by the analyst is appropriate. The framework obviates the need to make the application fit the pre-selected HRA method to be used.

In addition to developing NUREGs -1792 and -1842, the NRC is collaborating with the Electric Power Research Institute (EPRI) to pursue a consensus approach to HRA (Parry et al., 2011). The aim of the work is to develop an approach capable of modeling and quantifying human failure events in an adequate, reliable, consistent, and efficient manner. To develop such a "consensus HRA approach," the collaborators conducted thorough literature search to establish a technical HRA basis on the state-of-the-art of cognitive and behavioral science and a causal analysis aiming to be technology neutral.

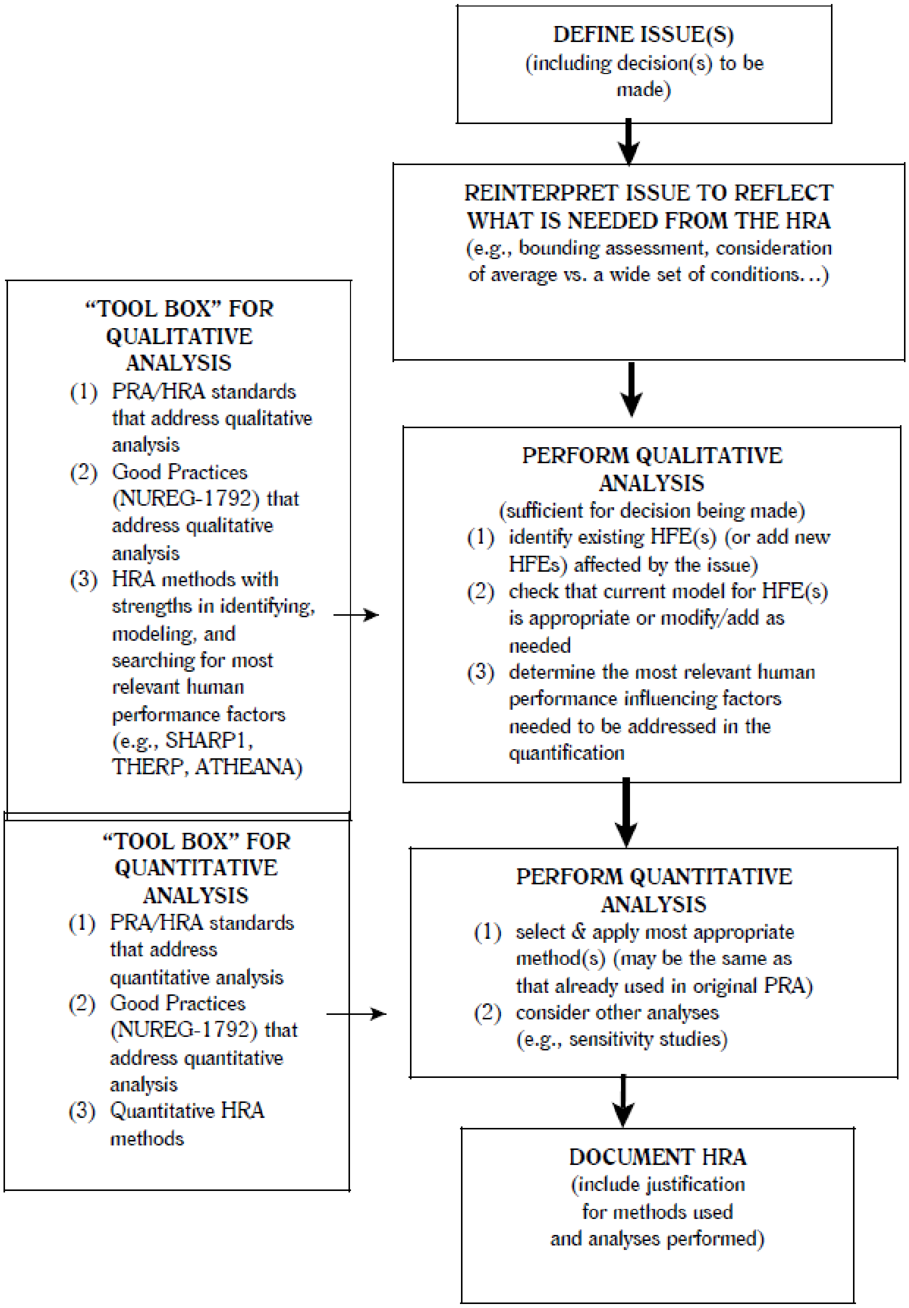
DEFINE ISSUE(S)
(including decision(s) to be made)
REINTERPRET ISSUE TO REFLECT WHAT IS NEEDED FROM THE HRA
(e.g., bounding assessment, consideration of average vs. a wide set of conditions…)
"TOOL BOX" FOR QUALITATIVE ANALYSIS
(1) PRA/HRA standards that address qualitative analysis
(2) Good Practices (NUREG-1792) that address qualitative analysis
(3) HRA methods with strengths in identifying, modeling, and searching for most relevant human performance factors (e.g., SHARP1, THERP, ATHEANA)
PERFORM QUALITATIVE ANALYSIS
(sufficient for decision being made)
(1) identify existing HFE(s) (or add new HFEs) affected by the issue)
(2) check that current model for HFE(s) is appropriate or modify/add as needed
(3) determine the most relevant human performance influencing factors needed to be addressed in the quantification
"TOOL BOX" FOR QUANTITATIVE ANALYSIS
(1) PRA/HRA standards that address quantitative analysis
(2) Good Practices (NUREG-1792) that address quantitative analysis
(3) Quantitative HRA methods
PERFORM QUANTITATIVE ANALYSIS
(1) select & apply most appropriate method(s) (may be the same as that already used in original PRA)
(2) consider other analyses (e.g., sensitivity studies)
DOCUMENT HRA
(include justification for methods used and analyses performed)

Figure 2-1 Process for selecting and implementing HRA methods
Source: NUREG-1842 (Forester et al., 2006)

The past and present work to improve HRA and identify best practices focuses on existing operating reactors. No current HRA method has been developed specifically for SMRs, and any application of existing HRA methods to SMRs will likely require modifications to generalize from legacy applications to SMRs. One key aspect is the identification of human failure events that are applicable to SMRs. These human failure events are considered in the next section.

3 Human Failure Events for Selected SMR Human-performance Issues

In this section, we identify human failure events for selected SMR human-performance issues. They represent opportunities for human failure in SMRs and should be reviewed for relevance and risk significance in PRAs dealing with individual SMR designs. It is important to emphasize that providing a complete set of human failure events for SMRs in general is not feasible. There are multiple SMR designs, each of which has relatively unique performance considerations. Many potential design basis accidents are unique to specific SMRs as well. Given the lack of a common design across SMRs, we can expect human failure events that will need to be considered in HRA to be different for each.

The SMR human-performance issues (from Table 1-1 that are discussed in this section are:

- New Missions
- High Levels of Automation for All Operations and Its Implementation
- Staffing Levels
- Multi-unit Operations and Teamwork
- Passive Safety System
- Load-following Operations
- Novel Refueling Methods
- HSI Design for Multi-unit Monitoring and Control

For each issue, a description is provided based on the information in O'Hara, Higgins and Pena (2012). Then potential human failure events are identified based on the issue description. As noted earlier, our purpose is to illustrate the types of human failure events that may arise based on the issues. Thus we have not been exhaustive of the events that may be applicable. When applied to a specific design, HRA practitioners may consider additional human failure events.

3.1 New Missions

The primary mission of current U.S. NPPs is to safely generate of electrical power. Some SMRs are designed to accomplish additional missions, such as producing hydrogen and steam for industrial applications, e.g., heating or manufacturing. Demick (2010) describes these new missions for high-temperature, gas reactors (HTGRs) as follows:

> These applications include supplying process heat and energy in the forms of steam, electricity and high temperature gas to a wide variety of industrial processes including, for example, petro-chemical and chemical processing, fertilizer production, and crude oil refining. In addition to supplying process heat and energy the HTGR can be used to produce hydrogen and oxygen which can be used in combination with steam and electricity from the HTGR plant to produce, for example, synthetic transportation fuels, chemical feedstock, ammonia, from coal and natural gas.)

Achieving these missions will necessitate having new systems and personnel tasks, and possibly, added workload.

Currently, the NRC staff reviews hazards of nearby facilities, such as natural gas. For SMR licensing reviews, these may be onsite and be a mission of the plant.

Possible human failure events for this issue include:

- Operators do not detect a reactor system degradation in a timely way leading to a more serious condition because their attention is focused on collateral tasks associated with other missions.

- Operators do not perform an emergency task because their attention is focused on collateral tasks associated with other missions.

3.2 High Levels of Automation for All Operations and Its Implementation

Automation is key enabling technology for multi-unit operations. As crews are assigned more units to manage, automation must undertake tasks traditionally performed by operators. SMRs are no exception, and their degree of automation will be high as both normal and safety operations will be automated. The "automate all you can automate" philosophy often dominates programs for developing advanced reactors to improve their performance and decrease operational costs. However, there is a complex relationship between automation and human performance, which often fails to confirm common-sense expectations (O'Hara & Higgins, 2010). For example, expectedly high levels of automation will lower workload; instead, it shifts workload and creates other human-performance difficulties, including:

- change in the overall role of personnel that does not support human performance
- difficulty understanding automation
- low workload, loss of vigilance, and complacency
- out-of-the-loop unfamiliarity, and degraded situation-awareness
- difficult workload transitions when operators must assume control when automation fails
- loss of skills since automated tasks seldom are performed
- new types of human error, such as "mode" error[1]

The design of SMRs and their operations must address these potential problems.

Concerns about these negative effects of over automation increased the usage of more interactive automation implemented at different levels (see Table 2-1). In addition, flexible approaches to using different levels of automation in a single system are being explored. In adaptive automation, its level is dynamic and changes with the needs of personnel and plant conditions. Therefore, this approach may assist operators in managing changing attentional and workload demands in supervising multiple plants.

[1] Automated systems often have a variety of modes in which the inputs used and output provided differ. Operator inputs might have different effects, depending upon each mode's characteristics. Errors result when operators make inputs thinking the system is in one mode when it is in another.

The reliability of automation also is an important consideration in using it. As automation's reliability declines, operator's performance and trust in the automation is degraded

Table 2-1 Levels of Automation

Level	Automation Functions	Human Functions
1. Manual Operation	No automation	Operators manually perform all functions and tasks
2. Shared Operation	Automatic performance of some functions/tasks	Manual performance of some functions/task
3. Operation by Consent	Automatic performance when directed by operators to do so, under close monitoring and supervision	Operators monitor closely, approve actions, and may intervene with supervisory commands that automation follows
4. Operation by Exception	Essentially autonomous operation unless specific situations or circumstances are encountered	Operators must approve of critical decisions and may intervene
5. Autonomous Operation	Fully autonomous operation. System or function not normally able to be disabled, but may be manually started	Operators monitor performance and perform backup if necessary, feasible, and permitted

Note: Adapted from O'Hara & Higgins, 2010, Table 3-3.

SMR designs must find the right balance between automation and human involvement to assure plant safety, by determining the right levels of automation and flexibility to support operators in maintaining multi-unit situation awareness (SA) and managing workload- demands. In addition, the design of SMR automation should mitigate the types of human performance issues that are associated with high-levels of automation. Licensing reviews of SMRs must determine whether the applicant has reasonably assured the effective integration of automation and operators, and the design supports safe operations.

The NRC's HFE reviewers should pay special attention to applications of SMR automation that extend beyond those typically used in new reactors, since there is little experience with them.

Possible human failure events for this issue include:

- Operators do not monitor the automatic system and do not recognize that it has failed.

- Operators do not override automation because they fail to understand its degraded condition.

- Operators override automation because they do not trust that it is performing properly.

- Operators make the wrong response to a plant transient because they thought an automatic system was in one mode but it was in another.

- Operators do not respond in time to an automation failure due to high workload associated with manual tasks.

3.3 Staffing Levels

10 CFR 50.54m governs the minimum staffing levels for licensed operators in current plants; it has a table establishing the numbers of operators for one-, two- and three-unit sites. For a one-unit site, one senior reactor operator (SRO), two reactor operators (ROs), and a shift supervisor (second SRO) are required for an operating reactor. For a two-unit site, two SROs and three ROs are needed. A three-unit site needs three SROs and five ROs. The table does not cover sites with more than three units.

Most SMRs for which staffing information is available, propose staffing levels below these requirements and, therefore, an exemption from this staffing regulation is needed. For example, one SMR design anticipates assigning one reactor operator to monitor and control four units, each consisting of a fully integrated reactor and turbine generator. Drivers supporting this approach include the reactor's small size, it's simple, design, high-degree of automation, modern HSIs, and it's slow response to transients. Control room staffing for the baseline configuration of one SMR design consisting of 12 units encompasses three ROs, one SRO control room supervisor, one SRO shift manager, and one shift technical advisor (STA). Thus, the staffing levels needed to safely and reliably monitor and control SMR units must be determined and reviewed, possibly addressing new positions and staffing models.

Possible human failure events for this issue include:

- Operators do not notice a process failure because low staffing levels result in high workload.

- Operators do not properly respond to a unit failure because needed support personnel are not available.

3.4 Multi-unit Operations and Teamwork

For many SMR designs we examined, a single crew/operator will simultaneously monitor and control multiple units from one control room. Key issues in effectively and reliably accomplishing this task will be teamwork, situation awareness (SA), control room and HSI design, and the operator's workload. Maintaining sufficient SA of multiple SMRs may tax crews and individual operators. For example, studies found that operators of unmanned vehicles sometimes focus on a particular vehicle and neglected others, or fail to notice important changes to them.

When operators are focused on a particular problem in current plants, other operators undertake their tasks. Such cooperation may be problematic when each operator is responsible for multiple units. In the oil refinery facility, this situation was resolved augmenting the crew with additional staff during times of high workload or special evolutions. This is a different operational practice than that in present-day control rooms where the on-shift crew manages all aspects of the plant's condition (except accidents).

Maintaining SA may be further challenged when other situational factors intervene:

- individual units can be at different operating states, e.g. different power levels or different states such as shutdown, startup, transients, accidents, refueling and various types of maintenance and testing

- unit design differences often exist

Shift turnovers occur two to three times a day when a new crew relieves the old crew. An effective way is needed to convey the status of each plant, ongoing maintenance, and trends in operation from one crew to another, particularly because more than one plant is involved, and one operator will be operating multiple plants.

Understanding the contribution of situational factors such as these to multi-unit monitoring and control tasks will be important in safety reviews.

Possible human failure events for this issue are:

- Operators do not notice a unit failure because they are monitoring other units.

- Operators do not take a necessary action because of loss of situation awareness of the failing unit.

- Operators take an emergency action required on Unit A on Unit B, thus committing an error of omission for Unit A and error of commission for Unit B (analogous to a wrong-unit, wrong-train error).

- An operator error is not identified through peer checking because individual units are monitored by only one operator.

- Operators take an wrong action because they were unaware of maintenance has taken a system out of service because the information was overlooked during shift turnover due to the amount of information that needed to be communicated.

3.5 Passive Safety Systems

Like some new reactor designs, SMRs employ passive safety systems to respond to transients and accidents that depend on physical processes rather than active components, such as pumps. For example, should an excessively high temperature be reached, the temperature gradient increases natural circulation. Many passive systems use one or two valves to initiate the process; the valve(s) must be highly reliable.

The International Atomic Energy Agency (IAEA, 2009) identified several concerns about passive systems based on the limited experience with reactor design using such systems:

- The reliability of passive safety systems may not be understood as well as that of active ones.

- There might be undesired interaction between active and passive safety systems.

- It may be difficult to ‘turn off’ an activated passive safety system after it was passively actuated.

- Implications must be proven of incorporating passive safety features and systems into advanced reactor designs to achieve targeted safety goals; supporting regulatory requirements must be formulated and established.

We note that passive safety systems depending of physical processes are not as amenable to routine testing as are active ones. There are no components to easily test, e.g., no pumps to start. For passive systems with valves, operating them would not fully test the process in the absence of the physical condition that initiates it. Thus, operators may not become as familiar using them as they are with current-generation active systems, nor know from operational experience how to verify the system's proper automatic initiation and operation in a real event. For example, there may not be the same observable initiation signals to start systems. Flow rates and temperatures typically are much lower, and perhaps not as easily verified.

Operational aspects of monitoring and verifying the success of passive systems must be defined, along with any operator's actions needed to initiate or back them up should they fail to operate as designed.

Possible human failure events for this issue are:

- Operators do not take a recovery action during passive system failure because they do not detect that the system is not performing as it should.

- Operators do not intervene when necessary because of they lack sufficient knowledge about how the passive system performs.

3.6 Load-following Operations

Current day NPPs typically operate at 100% power and provide a base load to the utility's electrical distribution system, i.e., the plants produce electricity for the grid and other producers of electricity compensate for changes in demand. Clayton and Wood (2010) suggested that a base-load mode of operation may not suffice for SMRs that may have to cooperate with other sources of renewable energy whose production is variable because they depend on sun and wind.

Load following is an operating procedure that allows the power output generated by the NPP to vary up or down as determined by the load demanded by the distribution system. It entails more transients, so the plant can increase or decrease both reactor- and turbine-power in response to the external demand. In turn, this requires more actions from operators, and increased monitoring of the response of the automatic systems. In addition, for a multi-unit site, load following may entail the startup and shutdown of units to meet large changes in load demand. Hence, there is more opportunity for equipment failures and operator errors.

Vendors and plant owners, in conjunction with the NRC, will need to decide on the method to implement load-following, e.g.:

Method A – A load dispatcher contacts the NPP's shift supervisor for all changes.

Method B – A load dispatcher dials in requested change, and the NPP automatically responds, while the load dispatcher and RO/SRO monitor for the proper response.

Each of the two approaches has its own issues. Method A creates a greater workload and more distractions for the operators. While manual control of a single unit is well within an operator's capability, simultaneously controlling several may be much more difficult and lead to errors. Method B permits a person not trained in NPP systems and not licensed to change reactivity and power level in the reactor to do so. The NRC has not permitted plants to be operated by an automatic load-following scheme.

Such a change in operating methods might increase risk due to a higher frequency of transients, and should be evaluated via PRA techniques. Load following and the interface with smart grids will cause repeated startup and shutdown of multiple modules, which may challenge operations, and potentially give rise to higher failure rates for equipment and personnel.

Possible human failure events for this issue are:

- Operators do not notice a system failure leading to an emergency condition because of high workload associated with load following operations.

- Operators do not take actions to respond to a load-following automation failure because they do not notice it due to the changing conditions of the units.

- If Method B is used, operators and local dispatchers unknowingly take counter-acting actions and hence delay the necessary response to a transient.

3.7 Novel Refueling Methods

Several SMR designs refuel the reactor on-line or continuously. While there is international experience with such refueling operations, it will represent a new practice in the United States. Further, in some circumstances, specific approaches to refueling will be novel. For example, the current NuScale refueling concept is.

> There will be online refueling operations where the reactor to be refueled is detached from its mounting position and connected to a crane. The crane then moves the reactor to a refueling bay for disassembly and refueling. The reactor instrumentation is monitored through the entire process. There are four channels of instrumentation and control (I&C). When preparing to move the reactor, first one channel's cable connector is removed from the reactor and attached to the refueling bridge (RB). When the channel on the RB is verified to be reading properly, the second I&C channel is similarly transferred, and then in turn the 3rd and 4th channels are transferred. Control of this reactor is the responsibility of an SRO in the refueling area, not the main control room. One concept under consideration is having a 13th reactor, which would then be moved to replace the one being refueled. Then the reactor could be refueled while the other 12 are still maintaining the full power output of the station.

It is likely that a refueling crew will manage this operation. However, there still are interfaces with the operators of the primary reactor that should be considered, as well as the operations of the refueling crews.

A possible human failure event for this issue is:

- Operators do not take a necessary action leading to a unit failure because they are distracted by communications with the refueling crew of another unit.

3.8 HSI Design for Multi-unit Monitoring and Control

The detailed design of HSIs (alarms, displays, and controls) to enable a single operator to effectively manage one or more SMRs is an important feature. HSIs must enable monitoring the overall status of multi-units, as well as easy retrieval of detailed information on an individual unit. This need raises several questions. For example, should the HSIs for with each unit be separate from those of other units, or should they be integrated to help operators maintain high-level awareness of the status of all units for which they are responsible. If the units are separated, and an operator is focusing on one of them, awareness of the status of the other units may be lost. If the information is integrated, it might be a challenge to ensure that operators do not confuse information about one unit with that about the others.

Alarm design is especially important in ensuring that operators are aware of important disturbances, so minimizing the effects of change blindness and neglect.

SMR personnel may also require more advanced I&C and HSI capabilities to support their tasks. For example, systems that provide diagnostics and prognostics support to monitoring and situation assessment activities may be available. How personnel manage and understand these capabilities is an important consideration in overall personnel- and plant-performance.

The organization of information in supporting teamwork is another important HSI factor e.g., deciding what information crew members need to have access to individually, and as a crew, to promote teamwork. A key aspect to be researched is employing a large overview display in a control room with multiple operators, each controlling more than one unit. Its value here may not be so clear-cut and obvious as it is for a single unit's control room.

Another problem is the HSIs needed for shifting control for one unit from one operator to another.

Possible human failure events for this issue include:

- Operators do not notice a system failure because they are managing alarms on another unit and the alarm system did not integrate alarms.

- Operators take an action on one unit that should have been performed on another unit because they were not easily distinguished in the HSI.

- Operators do not take an emergency action because unit responsibility has been shifted from one operator to another.
-
- Operator fail to take proper actions due to their workload resulting from transients in multiple units at the same time.

4 Conclusions

No current HRA method has been developed or modified to specifically address SMRs. As SMR designs are finalized, work will be needed to adapt current HRA methods for SMRs or to create new methods with SMRs as the intended application. Recent efforts to improve HRA have identified best practices focuses on existing operating reactors. Any application of existing HRA methods to SMRs will likely require modifications to generalize from current applications to SMRs. One key aspect is the identification of human failure events that are applicable to SMRs. As part of addressing the human contribution to plant risk, HRA practitioners identify and quantify the human failure events that can negatively impact normal or emergency plant operations.

The purpose of this report was to identify how the results of our research on SMR human-performance issues can be applied to HRAs/PRAs for SMRs. To do so we used the issues to identify potential human failure events. The human failure events we have identified are based on the descriptions of the SMR human-performance challenges discussed in each issue. The human failure events are stated in generic terms; unlike the actual human failure events developed by HRA practitioners during PRA modeling for a specific plant design.

These human failure events can be used by HRA/PRA practitioners and NRC reviewers to ensure that pertinent SMR human performance issues are appropriately addressed in specific SMR PRAs and HRAs.

The results illustrated here can be generalized to identify additional human failure events for the issues discussed and can be applied to those issues not discussed in this report.

5 References

American Society of Mechanical Engineers/American Nuclear Society. (2009). *Addenda to ASME/ANS RA-S-2008, Standard for Level 1/Larger Early Release Frequency Probabilistic Risk Assessment for Nuclear Power Plant Applications* (ASME/ANS RA-Sa-2009). New York: American Society of Mechanical Engineers.

Clayton, D. & Wood, R. (2010). The role of Instrumentation and Control Technology in Enabling Deployment of Small Modular Reactors. In *Proceeding of the Seventh American Nuclear Society International Topical Meeting on Nuclear Plant Instrumentation, Control, and Human-Machine Interface Technologies* (NPIC&HMIT 2010). La Grange Park, Illinois: American Nuclear Society, Inc.

Demick, L. (2010). *Transforming the U.S. Energy Infrastructure* (IN/EXT-09-17436). Washington, DC: U.S. Department of Energy.

Forester, J., Kolaczkowski, A., Lois, E. & Kelly, D. (2006). *Evaluation of Human Reliability Analysis Methods Against Good Practices, Final Report* (NUREG-1842). Washington, DC: Nuclear Regulatory Commission.

IAEA (2009). *Design Features to Achieve Defense in Depth in Small and Medium Sized Reactors* (IAEA Nuclear Energy Series Technical Report No. NP-T-2.2). Vienna, Austria: International Atomic Energy Agency.

Kolaczkowski, A., Forester, J., Lois, E. & Cooper, S. (2005). *Good Practices for Implementing Human Reliability Analysis* (NUREG-1792). Washington, DC: Nuclear Regulatory Commission.

NRC (2009). *An Approach for Determining the Technical Adequacy of Probabilistic Risk Assessment Results for Risk-Informed Activities* (Regulatory Guide 1.200, Rev 2). Washington, DC: Nuclear Regulatory Commission.

O’Hara, J., & Higgins, J. (2010). *Human-System Interfaces to Automatic Systems: Review Guidance and Technical Basis* (BNL Technical Report 91017-2010). Upton, NY: Brookhaven National Laboratory.

O’Hara, J., Higgins, J., & Pena, M. (2012). *Human Factors Engineering Aspects of Small Modular Reactor Design and Operations* (NUREG/CR-7126). Washington, D.C.: U. S. Nuclear Regulatory Commission.

Parry, G., Forester, J., Groth, K., Hendrickson, S., Lewis, S. & Lois, E. (2011). Towards an Improved HRA Quantification Model. In *Proceedings of PSA 2011 -- the ANS International Topical Meeting on Probabilistic Safety Assessment and Analysis*. Illinois: American Nuclear Society.