U.S. DEPARTMENT OF ENERGY

PNNL-23478, Rev. 0
SMR/ICHMI/PNNL/TR-2014/01

Prepared for the U.S. Department of Energy
under Contract DE-AC05-76RL01830

An Updated Methodology for Enhancing Risk Monitors with Integrated Equipment Condition Assessment

P Ramuhalli
EH Hirt
GA Coles
CA Bonebrake
BJ Ivans, Jr.
DW Wootan
MR Mitchell

July 2014

Pacific Northwest
NATIONAL LABORATORY

Proudly Operated by Battelle *Since 1965*

DISCLAIMER

PACIFIC NORTHWEST NATIONAL LABORATORY
operated by
BATTELLE
for the
UNITED STATES DEPARTMENT OF ENERGY
under Contract DE-AC05-76RL01830

Printed in the United States of America

Available to DOE and DOE contractors from the
Office of Scientific and Technical Information,
P.O. Box 62, Oak Ridge, TN 37831-0062;
ph: (865) 576-8401
fax: (865) 576-5728
email: reports@adonis.osti.gov

Available to the public from the National Technical Information Service,
U.S. Department of Commerce, 5285 Port Royal Rd., Springfield, VA 22161
ph: (800) 553-6847
fax: (703) 605-6900
email: orders@ntis.fedworld.gov
online ordering: http://www.ntis.gov/ordering.htm

This document was printed on recycled paper.
(9/2003)

PNNL-23478, Rev. 0
SMR/ICHMI/PNNL/TR-2014/01

An Updated Methodology for Enhancing Risk Monitors with Integrated Equipment Condition Assessment

P Ramuhalli
EH Hirt
GA Coles
CA Bonebrake
BJ Ivans, Jr.
DW Wootan
MR Mitchell

July 2014

Prepared for
U.S. Department of Energy
Contract DE-AC05-76RL01830

Pacific Northwest National Laboratory
Richland, Washington 99352

Executive Summary

Advanced small modular reactors (AdvSMRs) are based on modularization of advanced reactor concepts. AdvSMRs may provide a longer-term alternative to light-water reactors (LWRs) and small modular reactors (SMRs) that are based on integral pressurized water reactor concepts. AdvSMRs are designed to incorporate multiple modules (which may or may not have shared components and structures) at a single location, comprising a full "plant." AdvSMR operation differs fundamentally from full-size plants because the smaller plants may be used for load-following or peak-demand power generation, instead of baseload generation. AdvSMRs are also being considered for dual-use, where process heat would be used for both electricity generation and another purpose such as hydrogen production or water desalination, shown in Figure ES.1.

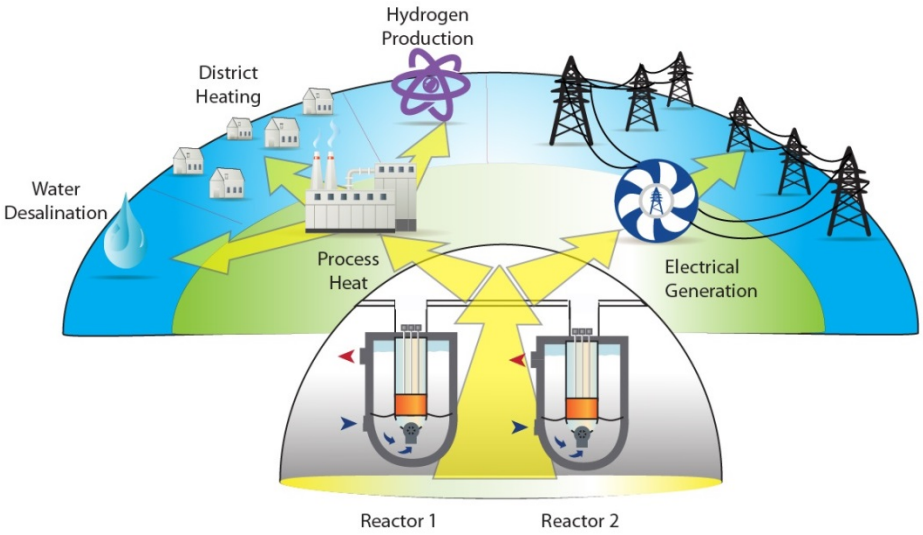

Figure ES.1. In Proposed AdvSMRs, Multiple Reactor Modules may be Co-located to Support Common Electrical Generation and Process Heat Applications

Enhancing affordability of AdvSMRs will be critical to ensuring wider deployment. Although some of the loss of economies of scale inherent to AdvSMRs can be recovered, the controllable day-to-day costs of AdvSMRs will be dominated by operation and maintenance (O&M) costs. A significant component of O&M costs is the management and mitigation of degradation of components due to their impact on planning maintenance activities and staffing levels. Traditional approaches to detecting and managing degradation such as periodic in-service inspections may have limited applicability to AdvSMRs, given the expectation of longer operating periods and potential difficulties with inspection access to critical components because of integrated and compact designs.

Technologies that help characterize real-time risk are important to controlling O&M costs and improving affordability of AdvSMRs. Component health and condition assessment coupled with predictive risk monitors can potentially ensure affordability of AdvSMRs through optimized operation planning and maintenance scheduling by:

- Maximizing generation through assessment of the potential impact of taking key components offline for testing or maintenance,
- Supporting reduced staffing needs by assessing the contribution of individual components to changes in risk and using this information to optimize inspection and maintenance activities, and
- Enabling real-time decisions on stress-relief for risk-significant equipment susceptible to degradation and damage, thereby supporting optimized lifetime management.

Given the possibility of frequently changing demand in AdvSMRs, techniques to integrate advanced plant configuration information, equipment condition information, and predictive risk monitors are needed to support real-time decisions on O&M (Coble et al. 2013). Essentially, enhanced risk monitors (ERM) are risk monitors that incorporate the time-dependent failure probabilities from prognostic health management (PHM) systems to dynamically update the risk metric of interest. In this, the ERM methodology differs from other approaches that incorporate aging models for key components. Rather than include generic aging models (for example linear aging models where the failure probability increases linearly over time), the ERM approach uses condition of the component to calculate the failure probability. Such systems may be applied at several levels in the hierarchy of AdvSMR systems. For example, component-level PHM systems may be applied to assess the condition of components or sub-systems, such as the intermediate heat exchanger. The use of multiple PHM modules provides increased opportunity to monitor the health of critical subsystems within the plant. However, it increases the amount of information that must be aggregated prior to use with risk monitors and in plant supervisory control actions. Figure ES.2 shows a possible scenario for the aggregation; where each PHM module is associated with a risk monitor resulting in predictive estimates of the subsystem health and the associated risk metrics. This information is used to augment data used for supervisory control and plant-wide coordination of multiple modules by providing the incremental risk incurred due to aging and demands placed on components that support mission requirements.

This report describes research results from an initial methodology for ERMs that integrate real-time information about equipment condition and probability of failure (POF) into risk monitors to provide an assessment of dynamic risk as plant equipment ages. This integration occurs at the level of the POF within risk monitors. The focus of the research presented here is on integration of sources of uncertainty into the ERM framework, and propagation of uncertainty through the ERM resulting in uncertainty bounds for the predicted risk metrics.

Risk monitors extend probabilistic risk assessment (PRA) frameworks by incorporating the actual and dynamic plant configuration (e.g., equipment availability, operating regimes, and environmental conditions) into the risk assessment. PRA is itself a systematic safety analysis methodology that follows four steps: (1) identify undesirable consequences (e.g., reactor unavailability, core damage) and initiating events that can lead to these consequences; (2) systematically identify accident sequences (defined by event trees and fault trees) through which the facility can move from the initiating event to the undesired consequence; (3) calculate the probability of occurrence for each accident sequence; and (4) rank the accident sequences according to probability of occurrence (or, alternatively, contribution to the undesirable event) to manage the major contributors to risk.

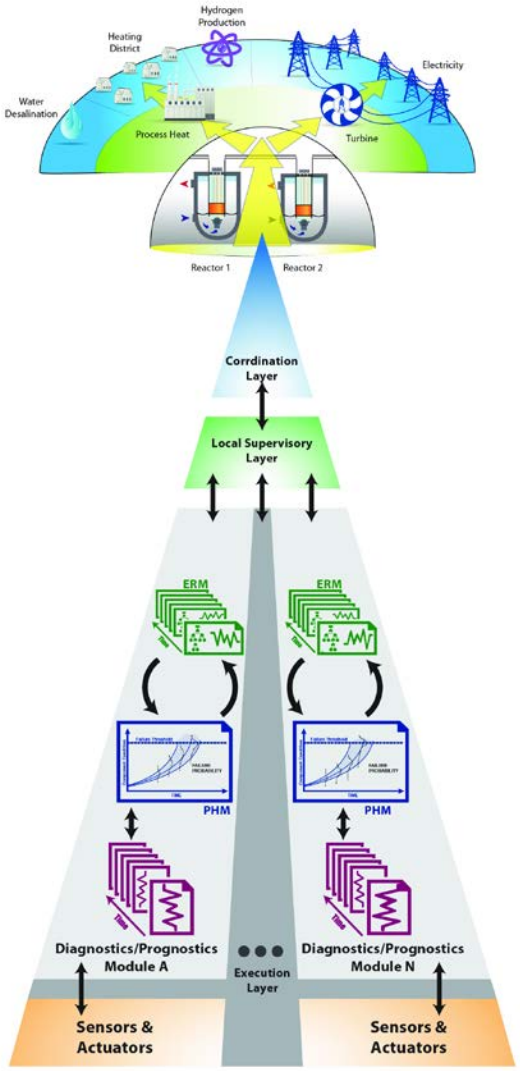

Figure ES.2. Schematic Showing the Integration of PHM Systems with Enhanced Risk Monitors, and Their Location within the Hierarchy of Supervisory Control Algorithms for AdvSMRs

For Level 1 PRA and associated risk monitors (which is the focus of the present work), the frequency of accidents that can cause core damage (called core damage frequency or CDF) is the risk metric that is typically used. Importance analysis is generally performed on the results of a PRA and provides a quantitative perspective on risk and sensitivity of risk to changes in input values.

Time-independence of component failures is assumed in traditional PRA modeling, and PRA component failure rates are typically assumed to be static over the life of the component. Changes (i.e., degradation) in the failure rate of a component that might be expected to normally occur over the component life are not explicitly represented.

The proposed methodology for ERM addresses this specific issue, and begins by defining PRA models that include all relevant components (based on failure modes and effects analysis that accounts for all potential operating conditions) and interdependencies between different modules of AdvSMRs. For

each of the relevant components, equipment condition assessment (ECA) methods are deployed to monitor the condition of the equipment and the surrounding environment. This information is used by a prognostic algorithm to predict the POF at a specified future time given the current condition of the component. As additional measurements become available (for instance, at successive time instants), the predictions may be improved by making use of updated condition information.

The component-specific time-dependent failure information (POF and confidence bounds) computed by the prognostics algorithm is then integrated into the PRA model, and the PRA model is solved to provide a time-dependent risk measure (such as CDF variation with time).

Uncertainty in PRA modeling arises from a number of sources that are typically divided into aleatory variability and epistemic uncertainty. Aleatory variability is related to the statistical confidence we have in failure probability data, while epistemic uncertainty is related to the uncertainty in the accident sequences used to develop the PRA model. In the context of ERM, several sources of uncertainty exist and result in uncertainty in both the equipment condition assessment and the predicted probabilities of failure. In turn, these uncertainties are expected to impact the predicted risk estimates from the ERM. In order to utilize the ERM results in a meaningful manner, the various uncertainties will need to be propagated through the ERM methodology to produce estimates of uncertainty in the ERM output.

While conventional risk metrics (specifically core damage frequency or CDF) may be utilized in this framework, it is likely that the real value of ERMs is with respect to alternative risk metrics that address risk from an O&M perspective. However, O&M-based risk metrics will need to be balanced with safety metrics to ensure that plant performance and maintenance schedules can be optimized to reduce cost while staying within specified safety margins.

Preliminary results of integrating time-dependent component POF and associated uncertainties into a risk monitor for a simplified model of a liquid-metal-cooled AdvSMR design are described in this report, and used to identify key areas for further development of the ERM methodology. The results to date overall indicate the potential for using the ERM methodology for decisions on optimization of O&M practices.

The simplified model of an AdvSMR is intended to be prototypical and resembles proposed liquid-metal-cooled SMR designs. The design is defined at a simple level of abstraction but contains enough resolution and specific design elements to inform the development of a PRA model that, when quantified, produces a cogent set of results.

Using the enhanced risk monitor for the simplified AdvSMR design, with the associated time-based component failure information and assumed uncertainties in component condition and POF over time, we computed and analyzed the changes in CDF over time. The results indicate that, using the proposed framework for ERM, as the failure probabilities and failure rates change over time, the CDF changes over time.

The effects of propagating the uncertainty in POF through the ERM methodology are complex, and depend on whether the overall uncertainty grows the further in time risk is projected. Assuming that the uncertainty grows the further out in time the predictions are made, the uncertainty bounds for the risk metric are also shown to grow. However, as additional information becomes available (through perhaps a measurement that updates the condition information on one or more components), the overall uncertainty

in risk is seen to reduce under certain circumstances. This appears to depend on the contribution of the component to the overall risk (i.e., the "importance" of the component).

Repairs or replacements (bringing the components to as-new condition) reduce the risk, although aging of other components may still drive the overall risk higher. As well, we assume that the uncertainty associated with the component condition after repair or replacement is reduced. While this contributes to reducing the uncertainty bounds in the risk metric, uncertainty in the aging of other components may still drive the overall uncertainty higher as well.

These pieces of information, when compared to traditional PRA analysis, appear to provide useful information for scheduling maintenance activities based on actual degradation condition and consequent failure probabilities. Specifically, if thresholds may be set on the risk metric of interest, the projected risk and uncertainty bounds provide a mechanism for scheduling maintenance activities whenever the risk (plus uncertainty) exceeds the threshold.

Key to accurate uncertainty quantification within the ERM will be the ability to accurately identify failure probabilities of typical components used in AdvSMRs. Such reliability data is not readily available, and for AdvSMR concepts, may comprise data from instrumented test reactors that were operated between the 1970s and 1990s. Available data from such test reactors is being examined for applicability to this project.

The ERM can provide additional value through the development of alternative risk metrics. Metrics associated with quantities such as cost or losses due to lost generation or unanticipated plant shutdown may provide valuable insights into the tradeoffs associated with continued plant operation while maintaining adequate safety margins. To this end, alternative risk metrics associated with these quantities are being identified and will be evaluated next.

Ongoing and planned research is focused on evaluating alternative risk metrics (including the options described earlier) and the impact of uncertainty on these risk metrics. In addition, we anticipate integrating the ERM methodology with simulation tools that simulate advanced reactor/AdvSMR modules and the impact of component degradation on their performance to perform comprehensive evaluations of the ERM methodology. In addition, we will explore the possibility of evaluations using experimental data, and to this end, will continue to evaluate sources of relevant reliability data, including data from test reactors, and available test-beds.

Acknowledgments

The work described in this report was sponsored by the Small Modular Reactor Research and Development Program of the U.S. Department of Energy Office of Nuclear Energy. The authors gratefully acknowledge Ms. Kay Hass for her invaluable assistance in the technical editing and formatting of this report. The authors also thank the technical peer reviewers for their feedback and assistance in improving this report.

Acronyms

AC	alternating current
AdvSMR	advanced small modular reactor
CAFTA	Computer Aided Fault Tree Analysis (system)
CCF	common cause failure
CDF	core damage frequency
CREDO	Centralized Reliability Data Organization (component reliability database)
DOE	U.S. Department of Energy
ECA	equipment condition assessment
EM	electromagnetic
EPRI	Electric Power Research Institute
ERM	enhanced risk monitor
F-V	Fussell-Vesely
FFTF	Fast Flux Test Facility
HRA	human reliability analysis
ICHMI	instrumentation, control, and human-machine interface
JCS	Job Control System
LMR	liquid metal reactor
LWR	light-water reactor
NPP	nuclear power plant
NRC	U.S. Nuclear Regulatory Commission
O&M	operation and maintenance
ORNL	U.S. Department of Energy, Oak Ridge National Laboratory
PHM	prognostics and health management
POF	probability of failure
PRA	probabilistic risk assessment
PSM	planning and scheduling modules
RAW	risk achievement worth
RRW	risk reduction worth
RVACS	reactor vessel auxiliary cooling system
SCRAM	an emergency shutdown of a nuclear reactor
SGL	steam generator louver
SMR	small modular reactor
SSCs	systems, structures, and components
SWRPRS	sodium-water-reaction pressure relief system

Contents

Figures

Table

1.0 Introduction

Small modular reactors (SMRs) generally include nuclear reactors with electric output of ~300 MWe or less. This cutoff may vary somewhat but is substantially less than full-size plant output of ~600 MWe or more. Advanced SMRs (AdvSMRs) refer to a specific class of SMRs and are based on modularization of advanced reactor concepts. AdvSMRs may provide a longer-term alternative to traditional light-water reactors (LWRs) and SMRs based on integral pressurized water reactor concepts currently being considered.

Enhancing affordability of AdvSMRs will be critical to ensuring wider deployment. AdvSMRs will suffer from loss of economies of scale inherent in small reactors when compared to large (~greater than 600 MWe output) reactors. Some of this loss can likely be recovered through reduced capital costs through smaller size, fewer components, modular fabrication processes, and the opportunity for modular construction. However, the controllable day-to-day costs of AdvSMRs will be dominated by operation and maintenance (O&M) costs.

Technologies that help characterize real-time risk to safe and economic operation are important for controlling O&M costs and improving affordability of AdvSMRs. Component health and condition assessment coupled with predictive risk monitors can potentially ensure affordability of AdvSMRs through optimized operation planning and maintenance scheduling by:

- Maximizing generation through assessment of the potential impact of taking key components offline for testing or maintenance,
- Supporting reduced staffing needs by assessing the contribution of individual components to changes in risk and using this information to optimize inspection and maintenance activities, and
- Enabling real-time decisions on stress-relief for risk-significant equipment susceptible to degradation and damage, thereby supporting optimized lifetime management.

Risk monitors are used in current nuclear power plants to provide a point-in-time estimate of the system risk given the current plant configuration (e.g., equipment availability, operational regime, and environmental conditions). However, current risk monitors are unable to support the capability requirements listed above as they do not take into account plant-specific normal, abnormal, and deteriorating states of systems, structures, and components (SSC).

This report documents research that updated the enhanced risk monitor (ERM) methodology to account for uncertainty in the equipment condition assessment (ECA), the prognostic result, and the probabilistic risk assessment (PRA) model. These results (based on impacting active component O&M) are a step towards ERMs that, if integrated with AdvSMR supervisory plant control systems, can provide the capability requirements listed and meet the goals of controlling O&M costs.

Additionally, technologies for characterizing real-time risk provide a mechanism for compensating for the relatively small amount of long-term reliability data from advanced reactor components. Such information was primarily collected from components used in test reactors over a number of years, and is not easily accessible presently. Given that similar components are anticipated in proposed advanced reactor and AdvSMR concepts, the ability to monitor performance and characterize changes in operational risk in real-time can reduce the level of dependence on such performance data. In parallel,

proactively establishing a viable ERM methodology before AdvSMR component design specifications are established supports: (i) building in opportunities for automated monitoring (on-line and off-line) of those components for optimizing performance with respect to anticipated demands on these reactors; and (ii) improving the maintainability of components from the perspective of time-to-repair and component cost.

1.1 Research Objectives

This report describes research results from an initial methodology for ERMs by integrating real-time information about equipment condition and projected probability of failure (POF) into risk monitors. This methodology is described using a model of a liquid-metal-cooled, modular AdvSMR design (Appendix A).

It is anticipated that the ability to characterize uncertainty in the estimated risk and update the risk estimates in real-time based on ECA will provide a mechanism for optimizing plant performance while staying within specified safety margins.

The specific objectives of the research described in this report are:

- Develop and evaluate the ability to propagate uncertainty from one or more sources to the estimated risk.
- Evaluate the ability to dynamically update the ERM calculation based on real-time updates to information on equipment condition, and evaluate the potential for utilizing these calculations for increasing surveillance intervals for components.
- Examine the potential for tradeoffs between O&M-based risk metrics while staying within allowable safety margins during operation of the AdvSMR.

The focus of the ERM methodology described in this report is on an updated ERM methodology that accounts for uncertainty in the ECA, the prognostic result, and the PRA model based on active components in AdvSMRs that are included in risk monitors. Updated results (evaluating the propagation of uncertainty from various sources) of integrating time-dependent component POF into a risk monitor for the simplified-model AdvSMR design are described, and used to identify key areas for further development of the ERM framework.

1.2 Organization of Report

This technical report is organized as follows. Section 2.0 provides an overview of AdvSMR O&M concepts, health monitoring and ECA for nuclear power components, and the role of ERM in AdvSMR control and coordination. Technical assumptions that were made during the development of the ERM methodology and its assessment are also documented. Section 3.0 describes ERM methodology and an assessment of results to date for the ERM methodology. Section 4.0 provides initial recommendations for interfaces between ERM and plant supervisory control. Section 5.0 summarizes ongoing and planned future research activities.

2.0 Background

The vast majority of nuclear power plant (NPP) operating experience involves light-water-cooled reactors and includes small LWRs. There is some experience with select advanced reactor concepts, which may be used to identify potential faults and failure modes for key components in AdvSMR concepts. Some of these issues are expected to be resolved in new AdvSMR designs (e.g., moisture intrusion through water-lubricated bearings may potentially be avoided by using sealed magnetic bearings), while other issues may still be relevant (though relevant data may not be easily accessible). These issues are likely to drive inspection and maintenance requirements for AdvSMRs.

Generally, AdvSMR concepts are distinguished from other NPP concepts by three factors:

- Using non-light water coolants—coolants being proposed for AdvSMRs include liquid sodium, lead or lead-bismuth eutectic, helium, and molten salt.
- Deliberately small in size—typically, AdvSMR concepts are expected to have electrical output less than about 300 MWe.
- Anticipated to be modular in configuration and operation, with one or more reactor modules in one power block, and multiple power blocks making up a plant.

Below, we briefly summarize advanced reactor concepts relevant to this research and provide background information on health monitoring, ECA, and PRA for nuclear power applications. This is followed by the technical assumptions that bound the research described in the rest of this document. Additional details of AdvSMR concepts and likely O&M approaches are provided in the previous reports in this series (Coble et al. 2013; Ramuhalli et al. 2013).

2.1 AdvSMR O&M Concepts

Leading AdvSMR designs are based on the advanced reactor concepts identified by the Generation IV International Forum (GIF) (Abram and Ion 2008), and include liquid-metal-cooled, gas-cooled, molten-salt, and supercritical water reactor concepts. Of these, the greatest amount of operating experience comes from liquid-metal-cooled and gas-cooled reactors. Both of these advanced reactor concepts have also been proposed in AdvSMR designs, and are likely to be closer to moving through the design and deployment cycle than AdvSMR concepts based on other coolant materials.

Details of advanced reactor concepts that are likely to be adapted for AdvSMR concepts are available in the previous report in this series (Coble et al. 2013). Additional background on other advanced reactor concepts and operational experience are available in the report on prototypic prognostic techniques for AdvSMRs passive components (Meyer et al. 2013a).

Several AdvSMR concepts use pool-type or integral configurations or very compact arrangements, which reduces accessibility to key components for frequent testing and maintenance. These designs are also expected to have fewer offline component testing and maintenance opportunities because of longer operating cycles between refueling. Additionally, modularity in AdvSMRs can, in some cases, introduce interconnections or dependencies between SSCs in reactor modules, resulting in event and failure trees that are very different from those present in current operating nuclear power reactors. Such

interconnections can impact overall risk in ways that are very different from current operating nuclear power reactors. Further challenging existing O&M practices is the expectation that AdvSMRs will operate in regimes that are removed from the current base-load generation regime. Thus load-following, reactor run-backs and load-balancing in multi-module reactors are all likely operational regimes for AdvSMRs. U.S. experience with these modes is limited and overseas operating experience suggests that these modes may result in added, potentially unanticipated, wear and tear on several components (such as control rod drive motors).

Health monitoring would provide condition indicators for key equipment using online, in-situ sensors and measurements to support detection and identification of incipient failure and to reflect evolving degradation. This is particularly important for SSCs proposed for use in AdvSMR designs that differ significantly from those used in the operating fleet of LWRs (or even in LWR-based SMR designs), as operational characteristics for these SSCs may not be fully available.

As discussed in Ramuhalli et al. (2013), the risk significance of active components in AdvSMRs may increase in spite of the greater reliance on passive mechanisms for safety goals. In combination with the potential for reduced access for testing and maintenance of in-vessel or in-containment components, this points to the need for greater condition monitoring of select active components with the goal of obtaining equipment condition in near real-time. Determining whether available condition monitoring techniques may be applicable to these components is a necessary step to leveraging existing technologies to the fullest extent possible.

2.2 Enhanced Risk Monitors for AdvSMRs

Advanced plant configuration information, equipment condition information, and risk monitors are needed to support frequently changing plant configurations (Yoshikawa et al. 2011). To utilize these three, often disparate pieces of information in making real-time decisions on O&M, approaches are needed to integrate these three elements in a manner that provides a measure of risk that is customized for each AdvSMR unit, and accounts for the specific operational history of the unit.

To achieve this integration, two separate technologies need to be integrated:

- Risk monitors (that currently are based on PRA models)
- Technologies for determining, based on the operational history and current configuration of the unit and its components, the present state of the component (for instance, "likely to continue operating within specifications," or "likely to fail soon with some probability," etc.). These are commonly referred to as diagnostic and prognostics technologies, in that they provide tools for the assessment of the current condition of SSC based on one or more measurements, and predict the operational condition at some defined time in the future based on the unit configuration and operational history.

The integration of these two technologies results in ERMs that use the real-time information on equipment condition to provide real-time updates to risk metrics. Essentially, ERMs would incorporate the time-dependent failure probabilities from prognostic health management (PHM) systems to dynamically update the risk metric of interest. In this, the ERM methodology differs from other approaches that incorporate aging models for key components. Rather than include generic aging models (for example, linear aging models where the failure probability increases linearly over time), the ERM

approach uses condition of the component to calculate the failure probability. Details of the ERM methodology are provided in Coble et al. (2013) and Ramuhalli et al. (2013), and are only briefly described here.

The general approach to achieving ERM is shown in Figure 2.1. The stages defined in this figure are related to identifying relevant SSC for which measurements are used to determine the current condition (ECA), and predict the condition (along with confidence levels in the prediction) at some point in the future (prognostics). The predicted condition, in the form of a POF is integrated into risk monitors, resulting in an ERM.

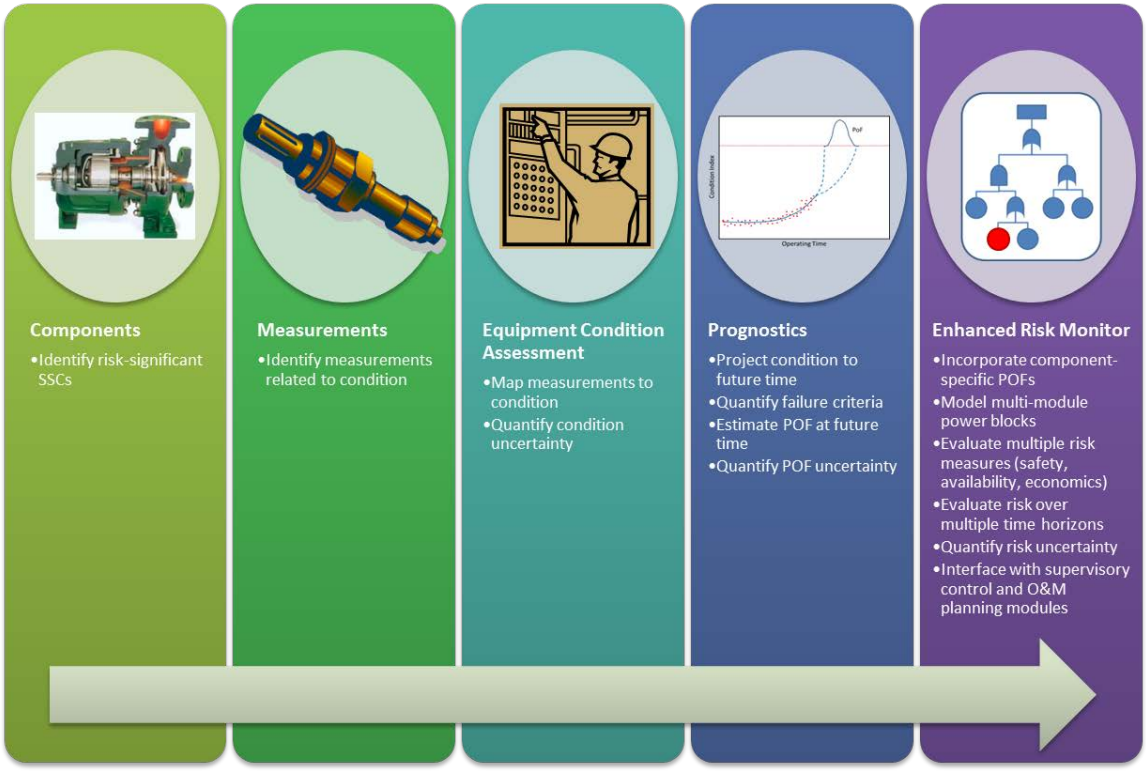

Figure 2.1. Considerations and Steps to Achieving an Enhanced Risk Monitor

The ability to predict (or estimate for future times) the POF based on equipment condition assessments and incorporate these in ERM may also help compensate for a relative lack of knowledge about the long-term component behavior of some components that are being proposed for AdvSMRs.

Relevant SSCs are generally those that are considered risk-significant, although this list can change as the plant configurations and operational conditions change. It is important to ensure that in determining relevancy such factors are considered. These key SSCs are then candidates for ECA.

2.2.1 PRA

Current risk monitors use PRA techniques that have been used in U.S. nuclear power plants to assess the risks associated with operation since the 1980s (Wu and Apostolakis 1992). PRA systematically combines event probability and POF for key components to determine the hazard probability for subsystems and the overall system (Kafka 2008). In general, PRA models use a static estimate for event probability and POF, typically based on historic observations and engineering judgment. More recently, time-based POF values have been used (Vesely and Wolford 1988; Arjas and Holmberg 1995); however, these are derived from operating experience and traditional reliability analysis and are usually not specific to the operating component.

While conventional risk metrics (specifically core damage frequency or CDF) may be utilized in this framework, it is likely that the real value of ERMs is with respect to alternative risk metrics that address risk from an O&M perspective. However, O&M-based risk metrics will need to be balanced with safety metrics to ensure that plant performance and maintenance schedules can be optimized to reduce cost while staying within specified safety margins.

2.2.2 Equipment Condition Assessment

ECA process measurements (e.g., flow, temperature, and pressure) or performance measurements (e.g., pump efficiency) are used as input to the ECA. Generally speaking, ECA methods rely on change detection techniques (Coble et al. 2013) to identify departure from normal operation and characterize the condition in terms of various condition indices. Challenges from the harsh environments in AdvSMRs may necessitate novel measurement methods, such as optical (Anheier et al. 2013) measurements of process parameters, or the use of sensors tolerant to these conditions (Daw et al. 2012).

2.3 Role of ERM in AdvSMR Control and Coordination

Given the possibility of frequently changing demands on AdvSMRs, techniques to integrate advanced plant configuration information and predictive risk monitors are needed to support real-time decisions on plant operations (Coble et al. 2013). Such information may be applied at several levels in the hierarchy of AdvSMR systems. For example, component-level PHM systems may be applied to assess the condition of components or sub-systems, such as the intermediate heat exchanger. The use of multiple PHM modules provides increased opportunity to monitor the health of critical sub-systems within the plant. However, it increases the amount of information that must be aggregated prior to use with risk monitors and in plant supervisory control actions. Figure 2.2 shows a possible scenario for the aggregation, where each PHM module is associated with a risk monitor resulting in predictive estimates of the subsystem health and the associated risk metrics. This information is used to augment data used for supervisory control and plant-wide coordination of multiple modules by providing the incremental risk incurred due to aging components and demands placed on those components to support mission requirements.

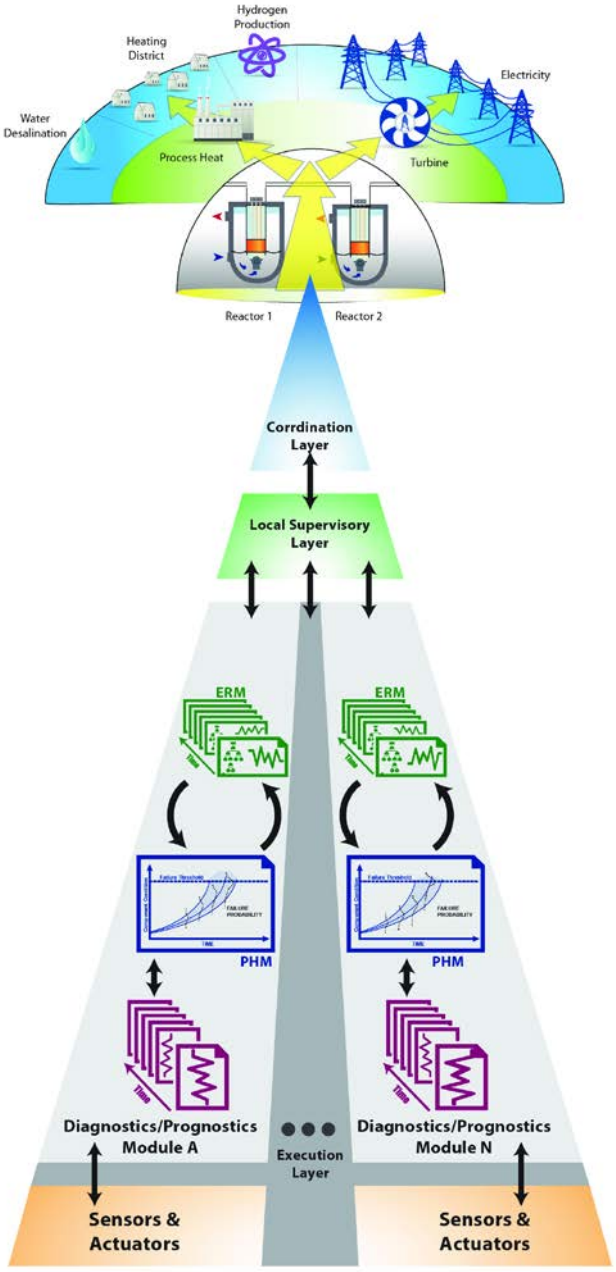

Figure 2.2. Schematic Showing the Integration of PHM Systems with Enhanced Risk Monitors, and Their Location within the Hierarchy of Supervisory Control Algorithms for AdvSMRs

2.4 Assumptions and Requirements for ERM Methodology Development in AdvSMRs

SMR/ICHMI/PNNL/TR-2013/02 (Coble et al. 2013) focused on the technical gaps in development of ERMs for active components in AdvSMR designs by integrating real-time information about equipment condition and POF into the risk monitor framework. This included defining a number of requirements for

enhanced risk monitors that integrate real-time estimates of equipment condition. These requirements were derived from expected operational characteristics of proposed AdvSMRs and include the ability to:

- integrate online, real-time ECA
- apply to multiple, interconnected modules and generation blocks
- evaluate risk over multiple time horizons
- apply condition-specific fault trees, event trees, and success criteria
- support reconfigurable balance-of-plant and fluctuating generation demands
- evaluate multiple risk measures
- meet runtime requirements for control and O&M planning.

A follow-up technical report (Ramuhalli et al. 2013) proposed a preliminary methodology for ERMs with ECA to address some of the technical gaps highlighted earlier. This ERM methodology addresses changes (i.e., degradation) in the failure rate of a component that might be expected to normally occur over the component life, and begins by defining PRA models that include all relevant components (based on failure modes and effects analysis that accounts for all potential operating conditions) and interdependencies between different modules of AdvSMRs.

This report describes progress towards increasing the realism of the ERM models through incorporation of uncertainty at several levels, particularly as available POF data is updated (nominally through the use of real-time condition assessment of key components).

2.4.1 Technical Assumptions

Several key assumptions are made in the development of the preliminary methodology for ERM that integrates time-dependent failure probabilities that are specific to the unit and the component condition. These are described in Ramuhalli et al. (2013), and are repeated below for convenience.

- The key aspects of the ERM methodology may be developed and initially assessed using a simplified model of an AdvSMR. In particular, we assume that the simplified model is of a liquid-metal-cooled AdvSMR.
- The focus of the ERM methodology described in this report is on active components in AdvSMRs that are included in risk monitors.
- Effective ECA techniques are assumed to be available for key active components and systems, including identification of the measurements necessary to perform ECA.
- Sensors for making the measurements needed for effective ECA are assumed to exist. These include measurements that are sensitive to component condition (such as vibration or current/voltage) as well as measurements of the operational environment (stressors). Ongoing research into sensors (such as that documented in SMR/ICHMI/PNNL/TR-2013/04 (Anheier et al. 2013) and Daw et al. (2012) will be leveraged where possible.

- We assume that existing prognostic algorithms will provide accurate extrapolation of equipment condition through future operation, as well as confidence bounds on the extrapolation; new approaches to prognosis are not a focus of this research. Investigations into PHM including risk assessment of passive components are covered separately as summarized in the report on prototypic prognostic techniques for AdvSMRs passive components (Meyer et al. 2013b). Developments in this area, with appropriate modifications to address active components, will be leveraged as needed.
- For the initial assessment of the ERM methodology, POF estimates at future time instants for the components identified in the simplified AdvSMR design are assumed to be available; however, the specific ECA technique and prognostic algorithm are not defined at this stage.

The development of the ERM methodology was also driven by the functional requirements for ERMs. These are briefly summarized next (details are in Coble et al. 2013). However, the preliminary methodology addresses only a sub-set of these requirements, with additional development necessary to address the other requirements.

2.4.2 Simplified-model AdvSMR Design

A simplified-model AdvSMR (power block) design is used in the development of the PRA model used for the research that supported the development of a framework for ERMs. This simplified model is shown in Figure 2.3, and details of the concept and its associated PRA model are presented in Appendix A. This hypothetical design is intended to be prototypical and resembles proposed liquid metal-cooled SMR designs. The example design is defined to provide a simple level of abstraction but contains enough resolution and specific design elements to inform the development of a PRA model that, when quantified, produces a cogent set of results.

The simplified-model AdvSMR design in Figure 2.3 is a small, modular, pool-type, liquid-metal-cooled reactor assumed to be producing 200 to 500 MWt[(a)] of power. The plant design consists of an unspecified number of identical power blocks, with each power block comprised of two reactor modules. Each module is connected to its own intermediate heat exchange system and steam generator. The secondary side (i.e., steam side) equipment is located in a different building and connects two modules to form a power block. A power block feeds a single variable capacity turbine generator. (*Note: While a greater number of reactor modules in a power block are possible, the present study restricts itself to two modules to develop and demonstrate a methodology for ERM.*)

(a) The electrical output of a reactor depends on the efficiency of the power conversion process.

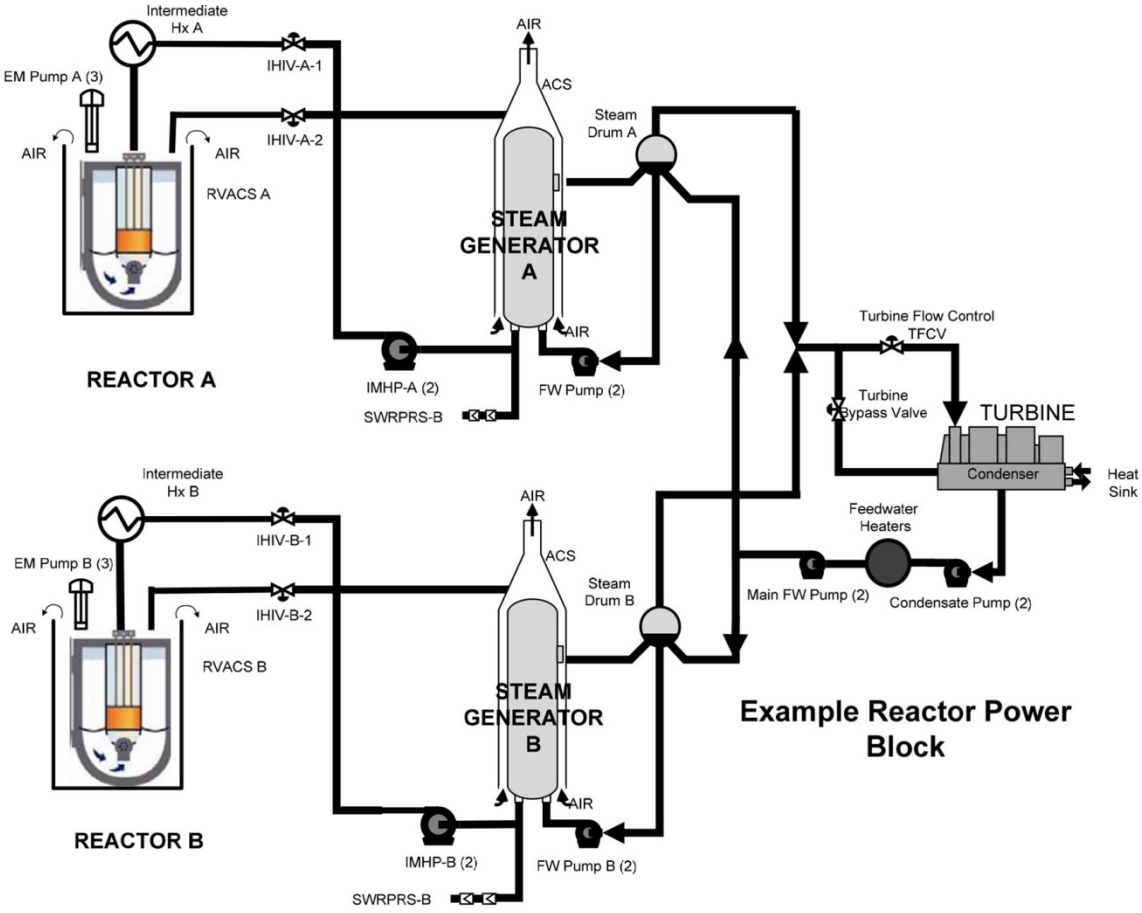

Figure 2.3. One-Line Diagram of Simplified-model AdvSMR

3.0 Assessment of Enhanced Risk Monitors

This section describes an initial methodology for enhanced risk monitors that integrate equipment condition assessment for dynamic characterization of system risk. The proposed methodology is applied to a risk monitor derived from the simplified AdvSMR design (Section 2.4.2 and Appendix A) and the results are described.

ECA is a requirement for ERM, and as discussed in Section 2.0, techniques for ECA are assumed to exist for the selected components of an AdvSMR. Thus, the state-of-the-art for ECA constrains the ability to deploy the ERM methodology and a better understanding of the state-of-the-art for ECA is needed before research needs for ECA of AdvSMR components may be defined.

This section begins by briefly describing the ERM methodology for the sake of completeness, including the general approach to integrating ECA/prognostics results with risk monitors. Factors impacting the ability to accurately assess risk in the ERM are then discussed. This is followed by an assessment of the ERM methodology as applied to the simplified AdvSMR design described in Section 2.4.2.

3.1 ERM Methodology

As described earlier, ERMs require integration of two sets of technologies—risk monitors and ECA/prognostics. In this section, we provide an overview of the approach to this integration.

Time-independence of component failures is assumed in traditional PRA modeling, and PRA component failure rates are typically assumed to be static over the life of the component. Changes (i.e., degradation) in the failure rate of a component that might be expected to normally occur over the component life are not explicitly represented.

However, experience has shown that aging of components generally results in time-dependent failure rates (Vesely and Wolford 1988). In reliability engineering, the failure probability is often defined to be a "bathtub" curve similar to that shown in Figure 3.1 (failure probability expressed as $\lambda(t)$ in the figure).

The ERM methodology that is being developed removes the fundamental assumption of static failure rates in risk monitors by integrating component-specific time-dependent failure probabilities that are calculated based on the current condition of the equipment.

We begin by defining PRA models that include all relevant components, as well as interdependencies between different modules of AdvSMRs. Component relevancy is determined by performing a failure-modes-and-effects analysis (FMEA) that takes into account all potential operating conditions (for example, full power steady-state operation, load-following, and reactor run-back). This information is used in the development of fault trees and event trees of the PRA model. These are solved to identify the cutsets that contribute most to risk.

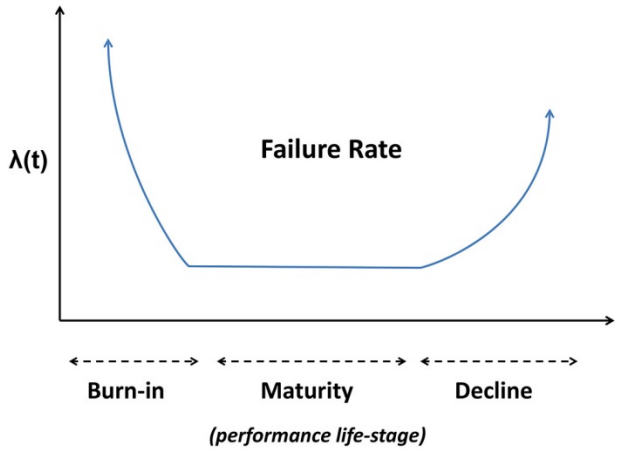

Figure 3.1. Generalized Component Failure Rate "Bathtub" Curve

For each of the relevant components, ECA methods are deployed to monitor the condition of the equipment and the surrounding environment. This information is used by a prognostic algorithm to predict the probability of failure at a specified future time given the current condition of the component. As additional measurements become available (for instance at successive time instants), the predictions may be improved by making use of updated condition information.

The component-specific time-dependent failure information (POF and confidence bounds as a function of time) is then integrated into the PRA model and the PRA model is solved to provide a time-dependent risk measure (such as the change in CDF with time).

Existing importance measures are based on the use of static failure rates, and may be less useful when applied to a model where failure rates and the calculated CDF change over time. A primary reason for this is the manner in which traditional importance analysis is generally performed; that is, through the use of ratios. This may be understood using a simple example. Risk achievement worth (RAW) is expressed as the ratio of the risk calculated with the element (e.g., basic event) always failed or unavailable to the baseline risk (Vesely et al. 1983). In the case where the baseline CDF changes with time (as does the POF), assuming a component is fully available does not change the time-dependency of the CDF (because other components are still assumed to have time-dependent POF values), although the values may be different from the baseline case. Because of division by small numbers taking ratios under these circumstances may result in large excursions in the risk reduction worth (RRW) that mask important details. Consequently, a failure event with a high-importance value at a given point in time might not be as important as a lower importance value at another point in time.

A more useful measure of importance must include consideration of the relative importance of the event to the total CDF as well as the value of total CDF itself. We proposed a new importance measure in Ramuhalli et al. (2013) in which the component failure of interest is set to a value of 1.0 (i.e., the component is assumed unavailable), the total CDF recalculated, and ratio of the CDF to a target CDF is calculated. This approach examines the relative increase in risk over the time-horizon of interest (when compared to a static or time-independent risk profile) due to the unavailability of a component. Other options for importance analysis may also be of relevance and will be investigated in the future.

3.2 Uncertainty Estimation in ERM

Uncertainty in PRA modeling arises from a number of sources that are typically divided into aleatory variability and epistemic uncertainty (EPRI 2011). Aleatory variability is related to the statistical confidence we have in failure probability data, while epistemic uncertainty is related to the uncertainty in the accident sequences used to develop the PRA model. Epistemic uncertainty is dealt with by developing event and fault trees as complete as possible, identifying keys sources of uncertainty, and performing sensitivity analyses. The aleatory variability is addressed explicitly by propagation of parametric data uncertainty for initiating basic event data. Uncertainty analysis is performed through a sampling strategy (e.g., Monte Carlo sampling) over some number of observations.

When incorporated in an ERM framework, several sources of uncertainty exist that directly impact the uncertainty analysis performed with PRA models. These include:

- Measurement noise
- Stochastic variability in stressors
- Manufacturing variability, leading to variability in failure rates
- Manufacturing defects that can lead to rapid failure of components (so-called infant mortality)
- Variability in degradation levels at which components fail

These sources of variability result in uncertainty in both the equipment condition assessment and the predicted probabilities of failure. In turn, these uncertainties are expected to impact the predicted risk estimates from the ERM. In order to utilize the ERM results in a meaningful manner, the various uncertainties will need to be propagated through the ERM methodology to produce estimates of uncertainty in the ERM output.

Methods exist to account for uncertainty in conventional risk monitors. However, as with component failure rates, these uncertainties are generally static and when propagated through the PRA models, result in static estimates of uncertainty.

A number of other mechanisms exist that can help study uncertainty propagation. Many of these methods, such as Latin Hypercube, are based on statistical sampling mechanisms. These techniques utilize models of the data that relate one or more explanatory variables to the observed data, and use probabilistic sampling mechanisms to propagate uncertainty.

In Ramuhalli et al. (2013), an initial assessment of sensitivity of ERM outputs to variation in component failure rates was performed. This was a limited assessment, with a small variability in the initial failure rates for one component was assumed and propagated forward through the ERM methodology. The approach assumed that the aging rate (or equivalently the rate at which the probability of failure of components increases with time) was unchanged. Results appeared to indicate that the small variation in initial failure rates resulted in a relatively small change in the CDF at future times, though the exact sensitivity was not quantified.

In this study, we explore this further. Specifically, we assume that mechanisms to quantify uncertainty in the various inputs exist and can be leveraged for uncertainty quantification in the component condition (based on the available measurements). Further, we assume that prognostic

techniques can also utilize statistical sampling approaches to quantify the uncertainty in predicted POFs. An example of this approach is particle filter-based prognostics, which can be used to estimate the uncertainty bounds for the predicted time to failure.

We then systematically vary the input uncertainty bounds and examine the impact on the predicted risk. To simplify the problem, we assume that the uncertainties are compounded over time (simulating the effect of increasing uncertainty in the POF with time), with the exact behavior of uncertainty with time (based on prognostic calculations) to be incorporated in the future.

3.3 Component Reliability Information from Existing Databases

As discussed earlier, AdvSMRs are expected to utilize components that, functionally, are similar to those used in currently operational and test reactors. For the purposes of calculating risk as a function of component degradation, baseline data on component failure rates are useful to bound the initial POF as well as expected failure rates as the component ages.

In the case of components on the secondary side, reliability data from currently operational plants may be used for this purpose, assuming that the secondary side of AdvSMRs is likely to serve similar functions (electrical generation, rejection of excess heat). However, several components are likely to be unique to advanced reactor concepts—components such as electromagnet (EM) pumps and intermediate heat exchangers. Reliability data on these components is limited. These data sets were primarily generated through the operation of a few test reactors, and with most of these test reactors no longer in operation, the accessibility of these data sets is greatly reduced.

To address this issue, two steps were taken. First, we began a systematic search of component reliability data that may be relevant to the generic liquid-metal cooled AdvSMR that is being used as a case-study for the ERM. Data that may be relevant from the Fast Flux Test Facility (FFTF) and EBR-II operation were collated into a database (Centralized Reliability Data Organization [CREDO] database) and efforts were initiated to assess the availability and relevance of the data. In parallel, similar data from other test reactors (such as N-reactor on the Hanford site) were also examined for availability and applicability. Details of these data sets, and the status of searches for the data, are described in Appendix B. In the interim, component failure rates from published literature (where available) were used to initialize the ERM for the generic AdvSMR design, and where unavailable, augmented with failure rates from like-kind components.

3.4 Risk Metrics for ERM

Risk metrics in PRA modeling are intended to capture the frequency of occurrence of undesirable consequences (e.g., reactor unavailability, core damage, release of radioactivity). A common metric in Level 1 PRA models (see Appendix A for definitions of PRA levels) is the frequency of accidents that can result in core damage (i.e., CDF).

While this is a useful metric for AdvSMRs and is used in this assessment, the increased reliance of these designs on passive safety features is likely to result in very low CDF values that reduce the utility of this particular metric. Instead, given the need to reduce O&M costs, metrics that capture the risk of plant unavailability to meet its mission needs (whether electrical generation or process heat or some

combination of the two) are likely to be of more relevance. In particular, such metrics provide a quantitative mechanism for understanding the impact to mission of the probability of component failure and consequent unavailability.

A number of publicly available reports and other documentation focus on the importance of managing nuclear power plant outages and equipment life and acknowledge the role of managing the condition of structures, systems, and components. While these documents are generally focused on operating experience from light water reactors, it is expected that similar concerns will be present with both advanced reactors and AdvSMRs, and lessons learned from the LWR community might help inform the development of alternative risk metrics that help advance the goal of safe and economic deployment of AdvSMRs.

The sources evaluated suggest that better optimization of nuclear power plant outages and equipment life management can significantly impact plant availability, operations, safety, and other costs associated with a nuclear power plant. Currently, each nuclear power plant develops its own strategy for short-term, middle-term, and long-term outage planning, although with AdvSMRs, it may be possible to standardize the maintenance planning across multiple, similar modules or plants. Extensive efforts are directed towards comprehensive planning of outages to minimize risks such as outage extensions, worker safety, radiation exposure, and plant unreliability (IAEA 2002). As for nuclear power plant and equipment life management, the economics of plant life management have become a crucial factor in being successful in competitive electricity markets (OECD 2000). Optimization of equipment monitoring, surveillance, and inspection using risk-based analysis have become increasingly important to optimizing equipment maintenance and life management. Given the competition from increased production of natural gas, the price of excessive outage extension or inadequate plant equipment management can lead to a facility that is no longer cost-effective to operate.

3.4.1 Outage Management Trends

Maintenance activities for currently operating reactors are generally managed during plant outages, which may be broadly organized into four groups based on the outage time (Kidd 2011):

- 7–10 days (refueling)
- 2–3 Weeks (refueling with standard maintenance)
- 1 Month (refueling with extended maintenance)
- Longer than a month (major back-fits or plant modernization)

Normally outages are planned well in advance, and involve replacement of fuel, and are optimized to minimize cost and duration. Planned outage management is very complicated because it must integrate the directives of the facility with available resources, safety, regulatory, and technical requirements. Component failure or even the threat of failure can force shut down of the plant for safety, operational, or regulatory reasons. According to (Kidd 2011), an unplanned outage is one of the worst situations for a plant, whether it occurs because of an unplanned SCRAM (an emergency shutdown of a nuclear reactor) of the reactor or for some other technical, safety, or regulatory reason.

A major objective for nuclear power plants is to avoid major unexpected repairs by having a proper spare parts policy based on a risk study (IAEA 2006). In the event of an unplanned outage, resources

have to be mobilized quickly, and are typically high-intensity, short-duration showdowns because refueling is not involved. In these cases, replacement power must also be purchased to meet the utility's power-generation obligations.

Over the last few decades utilities have spent significant resources on eliminating unplanned outages through increased equipment reliability and identifying the root cause of any unplanned events (IAEA 2006). As a result, unplanned outages have decreased significantly since the time frame prior to the Three Mile Island nuclear accident. The overall capacity factor for U.S. nuclear power plants has increased from 60% in 1980 to 90% today. Much of this increase was achieved by reducing outages, extending fuel cycles, using higher burn-up fuel, reducing unplanned outages, and reducing the number of fuel failures. Figure 3.2 shows the decrease in unplanned outages and SCRAMs from the 1970s to the 1990s (Miller et al. 2011). Also, the length of planned outages has decreased from 106 days in 1991 to 38 days in 2008 (Miller et al. 2011). Figure 3.3 shows this decrease in outage days.

However, though the current overall capacity factors for U.S. plants are quite good (90%), plant equipment problems and failures are by far the leading cause of unplanned outages (Nagatomi et al. 2010). Figure 3.4 illustrates this and also shows that outages due to plant or equipment problems are still a problem as they are major contributors to unplanned outages. So, although the nuclear power industry has made outstanding improvement, there is still a potential for decrease in unplanned outages that might be gained by better management of component condition.

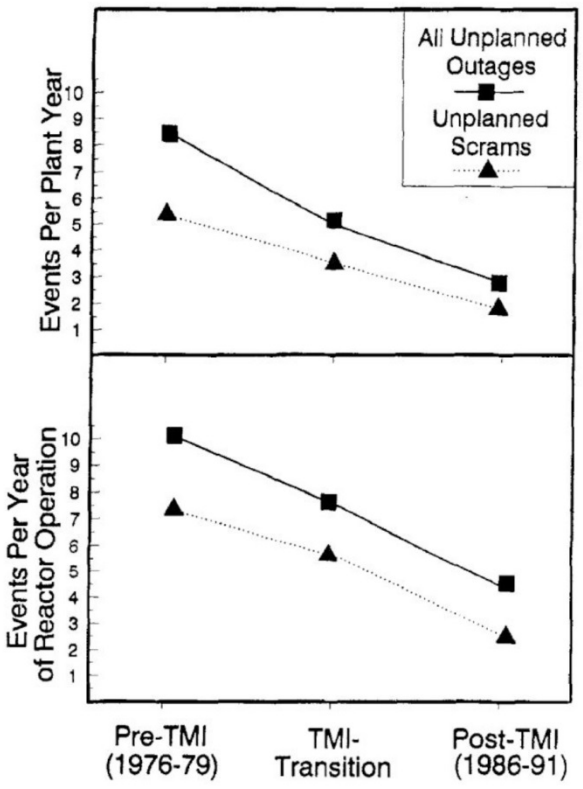

Figure 3.2. Unplanned Outages and Unplanned SCRAMs (David et al. 1996). Reprinted with kind permission from Springer Science+Business Media.

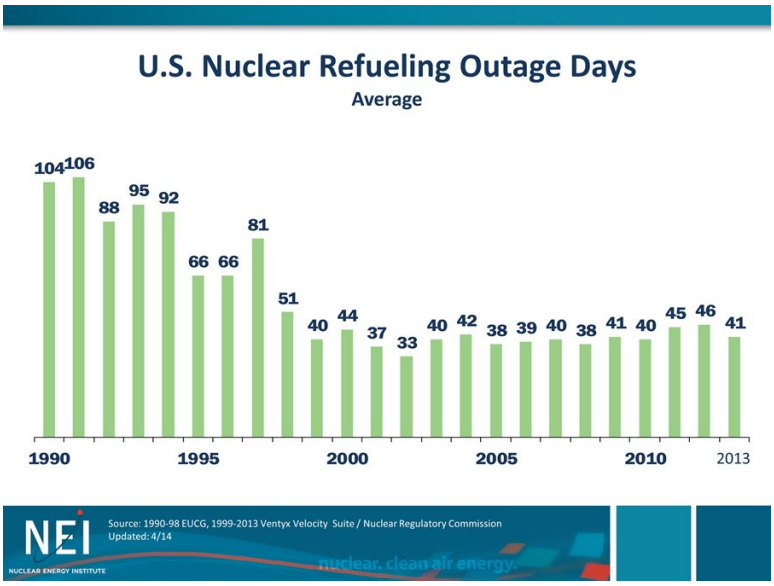

Figure 3.3. U.S. Nuclear Refueling Outage Days (NEI 2014). All rights reserved.

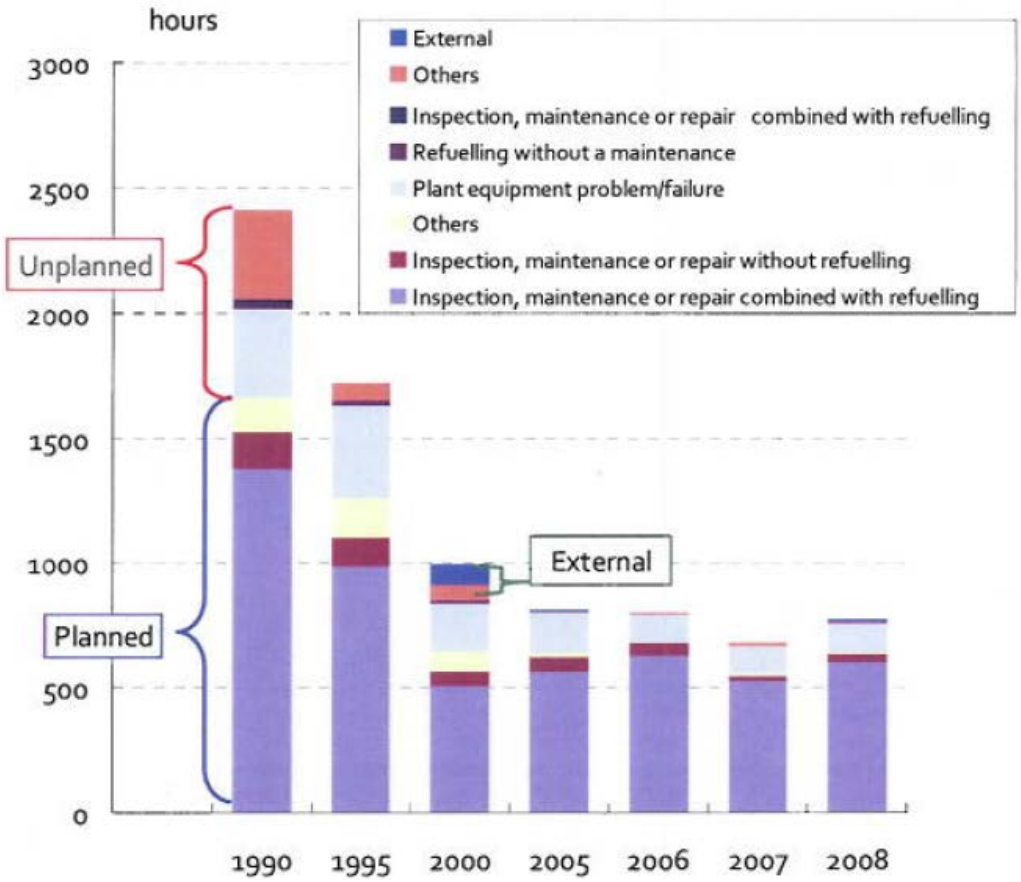

Figure 3.4. Average Outage Time by Cause in the U.S. (Nagatomi et al. 2010). Reprinted with permission from The Institute of Energy Economics, Japan.

3.4.2 Outage Management Needs

The IAEA suggests in their report on nuclear power plant outage optimization (IAEA 2002) that equipment failure types fall into one of three categories for plant life management: 1) critical components whose failure can influence the decision to retire a plant, 2) replaceable critical components whose failures needs to be avoided, and 3) non-critical components where run-to-failure might be an acceptable strategy. Figure 3.5 illustrates this categorization.

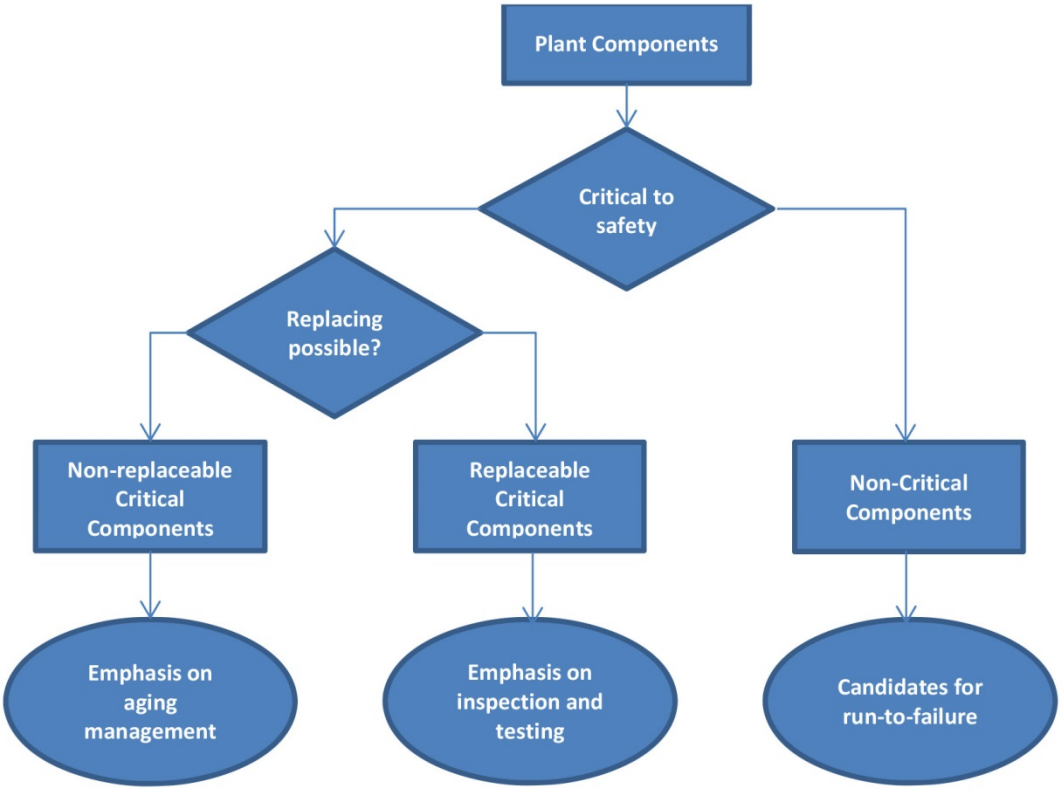

Figure 3.5. Component Categories for Plant Life Management (IAEA 2002)

The highest category of critical components are those whose failure can result in high replacement costs and bring into question the feasibility of continuing to operate the plant. These types of components might include the reactor vessel, steam generators, primary pumps, containment, and primary piping. Avoiding failure of these components is paramount and therefore aging management and controlling degradation are key activities. The second category includes components that are critical to the operation of the plant but typically have functional redundancy and are replaceable. Failure of these components could lead to extended outages, loss generation, and replacement costs. The emphasis for these components is testing, inspection, and preventive maintenance to avoid failures.

Certain systems are not critical to safety, reliability, or cost of operations. For these "non-critical systems," it might be economical to run them to failure. However, failure of these components might create conditions that trip the reactor leading to loss generation. This type of scenario is of particular

importance to AdvSMRs, where the interaction between modules may lead to conditions where failure of non-critical components may have unanticipated effects on the system as a whole.

This categorization of plant components illustrates the need to understand the criticality of a component to plant operation and nuclear safety and to manage the condition and life of the component accordingly.

3.4.3 Potential Risk Metrics to Support O&M Optimization

The increased importance of outage optimization and plant life management over the life span of nuclear power plants has resulted in the need for better tools and metrics to assist in associated decision making. As stated earlier, the use of alternative metrics along with CDF may provide quantitative insights to other risks of interest (e.g., cost of managing plant life) while showing that decisions made about outage management and equipment life maintain an acceptable level of nuclear safety.

The development of these metrics will require a study of the direct inputs to the ERM and the factors that influence these direct inputs. These direct inputs to ERM are:

- component failure rate
- component service life
- component mission time in an accident
- component test interval
- component repair time.

Factors that have the potential to impact these direct inputs include:

- maintenance practices
- maintenance intervals
- repair practice
- repair intervals
- inspection and test intervals
- component aging management policies (note that these may be informed by regulatory guidance)
- spare parts inventory
- equipment condition monitoring.

These influential factors represent the tradeoffs that define the O&M decision making, and therefore represent targets against which suitable risk-based metrics may be developed. Such metrics could include an array of concepts. Some of these are listed below (quantities in parentheses indicate measurement units in terms of cost and/or time offline):

- Number of unplanned outages due to equipment failure ($, days)
- Additional outage days because of equipment failure ($, days)

- Extended outage time ($, hours)
- Loss of electrical generation ($, days)
- Extended or permanent shutdown of the plant ($, days)
- Deferred equipment inspection ($, days)
- Reduced time for equipment inspection ($)
- Allowed outage time extension ($, hours)
- Extension of component life ($, years)
- Extension of plant life ($, years)
- Regulatory compliance ($, days)

Note that some of these metrics may need to be normalized appropriately (for instance, with respect to normal operations) to ensure that the metrics are appropriately bounded. A number of open questions will need answering before these metrics may be evaluated or used routinely. These include:

- Fraction of equipment replaced (perhaps unnecessarily) or repaired before it becomes a problem
- Cost ($, hours for maintenance, etc.) of equipment replacement/repair/maintenance during planned outages
- Approaches to prioritizing equipment for replacement/repair/maintenance during an outage
- Frequency of preventive maintenance and effort spent on preventive maintenance. Note that preventive maintenance may not necessarily need plant shutdown.
- Consequences of equipment failures (such as unplanned shutdowns), and the impact of mitigation strategies. For example, not all equipment failures may lead to unplanned shutdowns and there may be cases where the plant can bring online a spare to continue generating while repairs/replacements are made. In the latter case, however, there is likely to be additional effort (cost, resources) spent on replacement/repairs. Note that this may not show up as lost generation or loss of capacity factor although there is a cost associated with this.
- Average duration and cost of unplanned outages

3.5 Assessment of Updated ERM Methodology

The initial assessment of the ERM methodology uses PRA analysis of the simplified-model AdvSMR design depicted in Figure 2.3. The design only shows frontline components and supporting systems such as alternating current (AC) and direct current electrical power systems, instrumentation, and the details of the reactor trip system are not shown in the figure. Unlike the assessments described in previous reports (Ramuhalli et al. 2013), the PRA model used in the evaluations in this document incorporates additional details, including supporting systems and instrumentation as well as the reactor trip system. A list of the dominant cutsets from this PRA is provided in Appendix A, Section A.3.7.

3.5.1 Simplified-Model AdvSMR PRA

The PRA developed for the simplified-model AdvSMR is capable of modeling fault (or accident) sequences that could occur, induced by a perturbation (or initiating event) in the system, and of identifying the combinations of system failures, support system failures and human errors that could lead to core damage. The general framework for the PRA discussed herein includes the following analyses, each of which are discussed in detail in Appendix A:

- Initiating Event Analysis
- Accident Sequence Analysis
- Systems Analysis
- Data Analysis
- Common Human Reliability Analysis
- Cause Failure Analysis
- Quantification

A list of the dominant cutsets that account for over 97% of the total CDF (calculated using the analyses listed above and assuming static POF) is shown in Appendix A, Section A.3.7. The full list is used as the input to the ERM model.

The following success criteria are implicit to the defined cutsets:

- Four out of six control rod units, one out of four trip sensors, one out of four SCRAM breakers, and accurate trip setpoints are required for each module.
- The turbine bypass valve is required to open for one or two modules.
- One out of two main feedwater pumps is required for one or two modules. Both pumps are assumed to be running.
- One out of two module feedwater pumps is required for each module. Both pumps are assumed to be running.
- One out of two main condensate pumps is required for one or two modules. Both pumps are assumed to be running.
- One out of three electromagnetic pumps is required for each module. Two pumps are assumed to be running, and one is assumed to be in standby.
- One out of two intermediate loop pumps is required for each module. Two are required in case of an intermediate heat exchanger tube rupture. Both pumps are assumed to be running.
- The steam generator louvers (SGLs) are required to open for each module.
- In case of a steam generator tube rupture, either both the intermediate loop isolation valves or the sodium-water-reaction pressure relief system (SWRPRS) is required to prevent a loss of coolant accident from the reactor vessel, which would make reactor vessel auxiliary cooling systems (RVACs) ineffective.

- Sufficient heat (i.e., to prevent core damage) must be transferred from the reactor vessel to the containment vessel by radiative heat transfer and then to the air around the containment vessel and ultimately the atmosphere via convective heat transfer.
- For failure of RVACS caused by external events such as high winds, the opportunity for recovery (e.g., unplug radiating fins) by plant operators was assumed to be possible.

These success criteria are summarized in Table A.2.

Table 3.1 presents the initiating event and system component failure probabilities used to initialize the model (i.e., the failure probabilities when the components are as-built). Some components in this listing actually represent systems, such as RVACS, while others represent components.

Table 3.1. Initiating Event Frequencies and Component/System Failure Rates used in the Model

Component and Failure Mode	Failure Rate	Initiator or System Failure	Assumption/Comments
Electromagnetic Pump (Failure to Run)	3.00E-05/hr	Both	Assumed unproven for NPP use. Failure rate somewhat higher than average.
Electromagnetic Pump (Failure to Start)	3.34E-03/dmd	System Failure	Assumed unproven for NPP use. Failure rate somewhat higher than average.
RVACS (Failure to Operate)	5.00E-07/hr	Both	Recovery of RVACS given it plugs was assumed to be 1E-1.
Intermediate Heat Exchanger (Tube Rupture)	8.70E-03/yr	Initiator	Assumed unproven for NPP use. Failure rate much higher than average.
Intermediate Loop Isolation Valve (Failure to Close)	7.00E-03/dmd	System Failure	Assumed to somewhat higher than NPP average. Motive power undefined.
Intermediate Loop Pump (Failure To Run)	2.00E-05/hr	Both	Failure rate assumed to be near NPP average for motor driven pumps.
Steam Generator (Tube Rupture)	8.76E-04/yr	Initiator	Assumed to be proven for NPP use. Failure rate lower than average.
SWR Pressure Relief System (Failure to Operate)	2.00E-04/dmd	System Failure	Failure rate assumed to be near NPP average for pressure relief systems.
Steam Drum	-	-	Failure of this passive component not modeled. Assumed to be small contributor to risk.
Feedwater Pump (Failure To Run)	1.00E-05/hr	Both	Failure rate assumed to be near NPP average for motor-driven pumps.
Steam Generator Louver (Failure To Open)	5.00E-02/hr	System Failure	Bounded by operator failure to open steam generator air flow louvers.
Turbine Generator	-	-	Assumed to be encompassed by reactor transient trip events.
Turbine Bypass Valve (Failure To Open)	1.00E-03/hr	System Failure	Failure rate assumed to be near NPP average.
Turbine Flow Control Valve	-	-	Assumed to be encompassed by reactor transient trip events.

Component and Failure Mode	Failure Rate	Initiator or System Failure	Assumption/Comments
Main Feedwater Pump (Failure To Run)	1.00E-05/hr	Both	Failure rate assumed to be near NPP average for motor-driven pumps.
Main Feedwater Heater	-	-	Assumed to be encompassed by reactor transient trip events.
Main Condensate Pump (Failure To Run)	1.00E-05/hr	Both	Failure rate assumed to be near NPP average for motor-driven pumps.
Emergency Diesel Generator (Failure To Start)	4.53E-03/ dmd	System Failure	Failure rate assumed to be near NPP average for emergency diesel generators.
Control Rod Drive Mechanism (Independent Failure)	5.78E-06/ dmd	System Failure	Failure rate assumed to be near NPP average for control rod drive mechanisms.
Trip Sensor (Independent Failure)	2.00E-15/ dmd	System Failure	Failure rate assumed to be near NPP average for trip sensors.
Trip Circuit Breaker (Independent Failure)	2.00E-16/ dmd	System Failure	Failure rate assumed to be near NPP average for trip circuit breakers.
Trip Setpoint (Independent Failure)	3.00E-15/ dmd	System Failure	Failure rate assumed to be near NPP average for trip setpoints.
Emergency Diesel Generator (Failure To Run During First Hour)	2.90E-03/ dmd	System Failure	Failure rate assumed to be near NPP average for emergency diesel generators.
Emergency Diesel Generator (Failure To Run)	8.48E-04/ dmd	System Failure	Failure rate assumed to be near NPP average for emergency diesel generators.
Motor Control Center (Failure to Operate)	4.34E-07/hr	System Failure	Failure rate assumed to be near NPP average for motor control centers.
Electrical Bus (Failure to Operate)	4.34E-07/hr	System Failure	Failure rate assumed to be near NPP average for electrical busses.
Circuit Breaker (Failure to Open/Close)	2.55E-03/hr	System Failure	Failure rate assumed to be near NPP average for circuit breakers.
Circuit Breaker (Spurious Operation)	1.71E-07/hr	System Failure	Failure rate assumed to be near NPP average for circuit breakers.
Motor-Operated Valve (Spurious Operation)	4.45E-08/hr	System Failure	Failure rate assumed to be near NPP average for motor-operated valves.
Reactor Transient (Trip)	2.50E-01/yr	Initiator	Failure rate assumed to be below average for NPP trips.

Note: Adapted from NUREG/CR-6928, Industry-Average Performance for Components and Initiating Events at U.S. Commercial Nuclear Power Plants (Eide et al. 2007).

For this preliminary analysis, where available, industry documented failure data (Eide et al. 2007) was used to define initiating event and component failure likelihoods for the key components in the simplified-model AdvSMR design. The first-year values were set to be compatible to mean industry failure rates presented in NUREG/CR-6928; however, latitude was taken in adjusting these values for the example. Specifically, for components where such data is not readily available, assumed failure data was used based on available operational experience and like-kind components.

Initial evaluation of the ERM incorporated assumed time-based event and failure probabilities for each of the initiating events and key components failures of our example AdvSMR power block. These time-based likelihoods assume that the probability of failure increases from the initial probability when

equipment is in like-new condition to a maximum probability of failure from component aging, until a scheduled maintenance action is taken. Periodic maintenance intervals are staggered for each component to reflect different operating lifetimes.

3.5.2 Updated Results for ERM Assessment

The risk measure used in this updated assessment is the CDF. As described in Ramuhalli et al. (2013), the time-varying POF for the components in any given cutset were used to obtain predicted CDF values for that cutset over the assumed 40 year lifetime of the AdvSMR. The total CDF is computed by adding the CDF from each cutset. As indicated earlier, in the ERM model, the failure rate for the "new" component was set to be comparable to an industry mean failure rate for like-kind components and the end-of-life failure rates were set to be comparable to the 90 percent failure rates for like-kind components. When a component is refurbished or replaced (during scheduled maintenance at the end of its nominal service life), the failure rate is returned to the initial value.

To assess the propagation of uncertainty in the ERM, uncertainty in the initial POF for each component was assumed. Further, the uncertainty is assumed to increase at a uniform rate as the POF is projected out in time. This assumption simulates a prognostic algorithm that projects POF and computes the associated uncertainty. While such algorithms are available (for instance, Ramuhalli et al. 2012), for the purposes of this study we utilize the simplifying assumption described above.

Given the uncertainty in the initial POF and the uncertainty in the projected POF, we propagate the uncertainty through the ERM at each time step to compute the associated uncertainty in the predicted CDF. Figure 3.6 shows an example of the total CDF, with the associated uncertainty, computed using this technique.

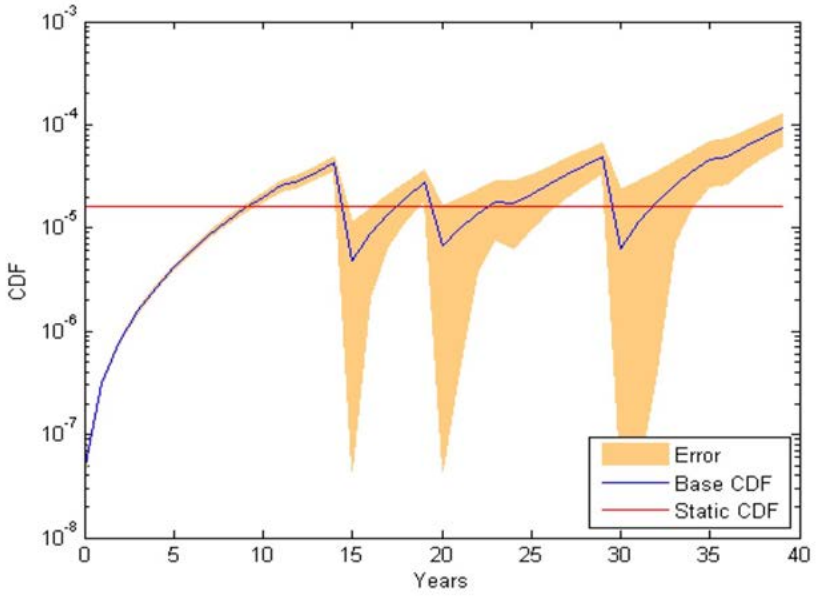

Figure 3.6. Projected CDF and Associated Projected Uncertainty Bounds due to Uncertainty in the Initial POF and Projected POF

As seen from Figure 3.6, the uncertainty in the CDF increases with time, until such time as a major repair or replacement activity is scheduled. At this stage, the component is assumed to be returned to like-new condition (either through a refurbishment or replacement) and the POF (and uncertainty) return to the original values. This results in a large drop in the lower uncertainty bound, although the upper bound is several orders of magnitude higher. This is attributed to the fact that the repair/replacement actions for the different components are not always synchronized, resulting in several components still contributing a higher uncertainty value.

Figure 3.6 also shows, for comparison, the CDF computed using a static POF estimate (horizontal line in figure). For the sake of comparison, the average POF (over 40 years) for each component is used in this calculation. If we were to assume that this quantity represents the acceptance criterion (i.e., the threshold beyond which the risk is considered unacceptable), the time at which the projected CDF exceeds this level would represent the time horizon for any potential interventional actions (repair/replacement scheduling). Note, however, that the uncertainty bounds result in timelines for intervention that are in advance of the time at which the projected CDF exceeds the threshold. This type of result indicates a need to tighten the uncertainty bounds as much as possible to increase the time horizon for repair or replacement actions.

The ERM keeps track of the dynamic values of a component's failure rate and updates these using ECA. Figure 3.7 shows an example of the updates to the predictive risk from the ERM based on ECA of one component (the steam generator louver) at 4 years and then again at 8 years. The ECA is assumed to indicate a better-than-expected condition of the component. For comparison, the predictive risk using only the information available at plant start-up is also shown. This update to the component condition due to an inspection is assumed to also result in a reduction in the uncertainty associated with the component POF. These new values of the POF and uncertainty are then used as the basis for projecting the risk metric (i.e., CDF) into the future (i.e., between the time of inspection and the end-of-life of the system—40 years in this example). Figure 3.8 shows the predicted CDF with uncertainty bounds. To better see the CDF and associated uncertainty, the predicted CDF is only shown out to 15 years. As seen from this particular example, the associated uncertainty in the risk metric decreases as the component POF uncertainty decreases, and then slowly increases again with time. This behavior is repeated with each additional update to the component POF. Figure 3.9 shows similar results, but with a higher level of uncertainty, and shows that the uncertainty in predictive risk is a function of the uncertainty in the inputs to the ERM.

This change in risk profile (and associated uncertainty bounds) is important from the perspective of defining a threshold above which the system is assumed to be in violation of its safety margins. Note that an ECA that indicates a component in better-than-expected condition results in a decrease in the overall risk metric (red curve in Figure 3.7). As a result, the consequences of continued operation of the plant using this component do not become significant (i.e., exceed the set threshold) until sometime later than estimated using the base case (no update to the equipment condition – blue curve). The incorporation of uncertainty in this context has an impact on the time at which the CDF exceeds the setpoint (Figures 3.8 and 3.9), and again point to the need to improve uncertainty estimates.

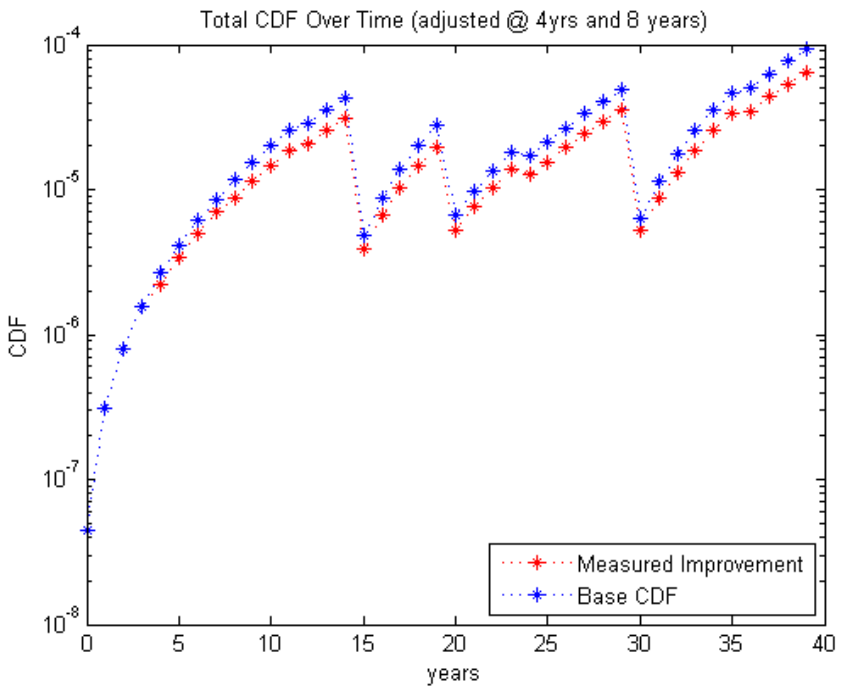

Figure 3.7. Change in CDF Based on Condition Assessment at 4 Years and 8 Years into Operation. The base case shows the predictive risk only using information at plant start-up.

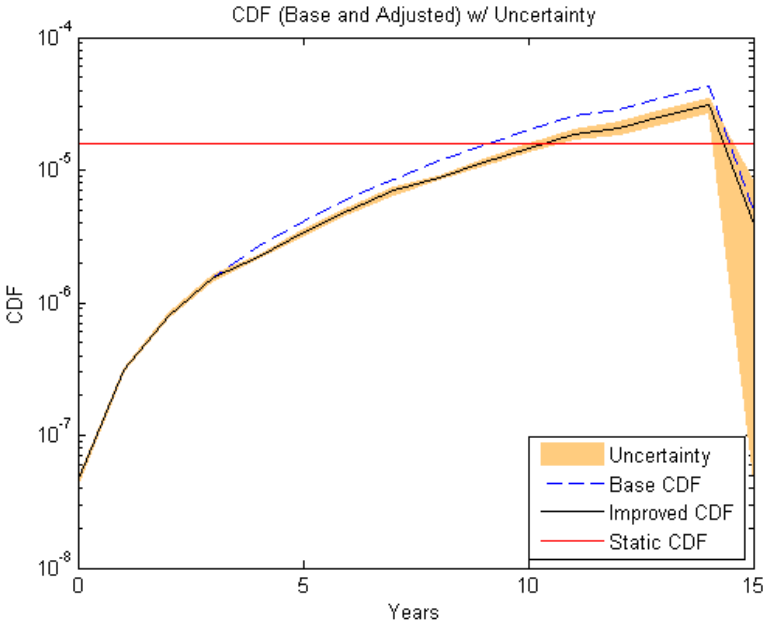

Figure 3.8. Change in CDF Based on Changes in Equipment POF, with Uncertainty in POF Assumed to Grow by 1% Each Year. Condition assessment of the steam generator louver is assumed to occur at 4 years and 8 years into operation of the plant.

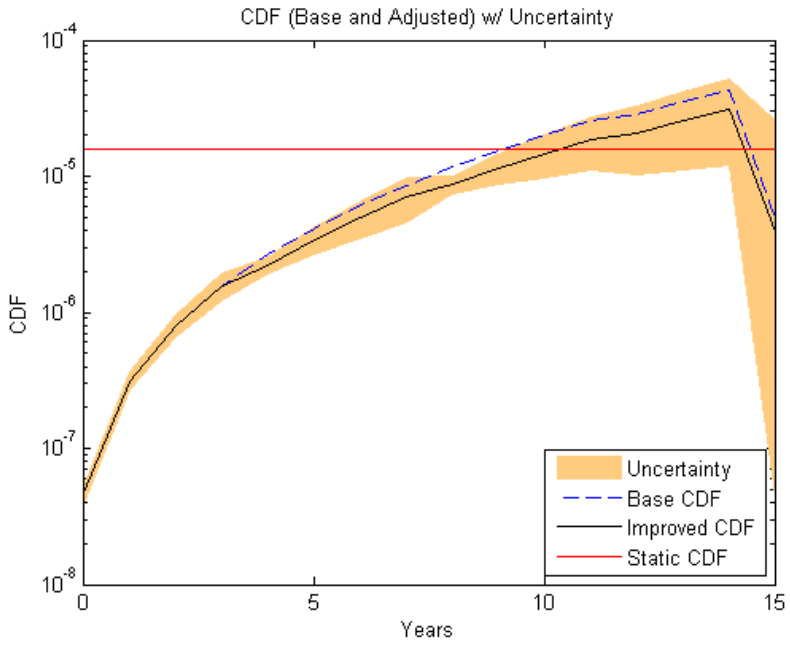

Figure 3.9. Change in CDF Based on Changes in Equipment POF, with Uncertainty in POF Assumed to Grow at 5% Each Year. Condition assessment of the steam generator louver is assumed to occur at 4 years and 8 years into operation of the plant.

The change in the risk profile is generally due to a change in the component POF. Such a change could be the result of an ECA, as discussed above, or due to an increment of surveillance test interval (STI) extension time. As a consequence, the ERM becomes a handy tool to perform what-if analyses, whereby the impact of delaying certain O&M actions may be defined. Applying increments of change associated with some alternate metric (i.e., a non-CDF metric) could also produce an increase in CDF rather than a decrease, such as might be the case for non-replacement or refurbishment of a particular component that has cost savings associated with the decision.

For determining the impact of surveillance test interval extension, the unavailability of the standby components needing surveillance tests must be estimated. The unavailability of standby components is based on standby failure rates, so their unavailability can be forecast as changing over time. The extent to which this extension contributes to CDF can be predicted a PRA model as static value, but is predicted as a dynamic value by ERM.

3.6 Discussion

The current approach to evaluating the risk associated with changing plant configurations does not adequately account for the actual degraded state of key components and structures. By incorporating real-time information about equipment condition, risk can be more accurately quantified, and O&M decisions and schedules can potentially be optimized. This is true as long as the uncertainty in the ERM inputs stays at a reasonable level. This is demonstrated by means of simplified PRA modeling of an AdvSMR and examining the changes in CDF over time as a result of the changes in failure probabilities over time of several key components. As these failure probabilities are updated, so are the predicted CDF over

time. The resulting information, when compared to traditional PRA analysis, appears to provide useful information for scheduling maintenance activities based on actual degradation condition and consequent failure probabilities.

As discussed in earlier reports (Ramuhalli et al. 2013), the initial analysis indicated that, using available component failure data, the overall CDF in the example PRA model was orders of magnitude smaller than those generally accepted for currently operating reactors. This is likely because of the small number of key components used in the PRA modeling as well as the use of passive safety features in AdvSMRs. However, this is an expected feature in AdvSMR PRA modeling, as typical risk measures such as CDF are expected to be lowered because of the inclusion of passive safety mechanisms. Although the CDF increases over time in the example presented in Figure 3.6 (and eventually exceeds levels generally accepted for operating reactors), it is because of a potentially inflated rate of change of the probability of failure over time.

When combined with the fact that enhanced fuels planned for use in AdvSMRs may preclude significant fuel failure, the ability to use CDF as a meaningful measure of risk may be reduced. New, non-traditional risk measures will need to be identified that support the economic and production goals of AdvSMRs, in addition to safety goals. A number of possible targets for the development of these nontraditional metrics were identified that appear to be relevant to the overall mission of improving availability of the AdvSMR modules while maintaining adequate safety margins (defined by CDF).

Along with identifying appropriate risk measures, criteria need to be established to assess the acceptability of plant configurations based on risk results (Puglia and Atefi 1995). Establishing acceptance criteria for different risk measures is an operational issue that will be considered in conjunction with the development of supervisory control and O&M planning algorithms, although site-specific acceptance criteria will likely need to be developed by utilities and regulators.

4.0 ERM and Plant Supervisory Control – Preliminary Interface Recommendations

As described in Section 2.3, techniques to integrate advanced plant configuration information and predictive risk monitors are needed to support real-time decisions on plant operations (Coble et al. 2013). This section briefly describes initial work towards defining interface recommendations for the ERM tools to interact with the Plant Supervisory Control logic. Note that, in this section, we assume that plant Planning and Scheduling Modules (PSM) are available. The PSM modules are expected to generate a partial schedule, work list, and parts list needed to restore the SSC during the next outage.

4.1 Brief Overview of Supervisory Control

The Supervisory Control for Multi-Modular SMR Plants Project is an effort led by Oak Ridge National Laboratory (ORNL) under the AdvSMR R&D Program to develop a new, state of the art overall control system intended to control O&M costs for multi-reactor plants to be in line with current LWR plant levels. Given the small output of each reactor, providing staff similar to current LWR practice would likely result in unsustainable O&M costs. The main overall goal is to allow operating the multi-reactor SMR plant with a staff size similar to a current generation LWR with similar total output; see SMR/ICHMI/ORNL/TR-2013/04 (Cetiner et al. 2013). The Supervisory Control system is planned for implementation as a non-safety system though it is required to not interfere with safety systems.

The output of the PSM is a schedule and work list for the next planned or unplanned outage (SMR/ICHMI/ORNL/TR-2013/04). Because an unplanned outage can start with very little warning, the PSM needs to frequently update this unplanned shutdown work list, a list of additional work that should be done if a given SSC failure causes a forced outage (additional work that can be done without interfering with the controlling path dictated by the "main" SSC repair work). This should include providing a list of materials and parts needed to do the work. It would be useful to the operations and maintenance staff for the PSM, on demand, to provide risk (success probability and/or PRA impact) for proposed on-line maintenance.

4.2 ERM Outputs

In general, the objective of interfacing the ERM to the supervisory control modules is to provide the control logic with a series of options that account for plant equipment condition and the risk to mission of operating the reactor given the current equipment condition. Equivalently, the risk to mission may be stated in terms of a probability of success ("success probability") given the current equipment condition.

In general, we expect that the ERM output will be utilized by the supervisory control logic as well as by the PSM module (for planning and scheduling maintenance actions). The ERM is expected to use predictive estimates of remaining life and POF from prognostic modules. At a minimum, the information provided by the ERM should be sufficient for each entity to perform its function. Specifically, the Supervisory Control logic should have sufficient information to be able to remove from service or reduce load on SSCs experiencing degraded condition, and the PSM should have sufficient information to generate a usable shutdown schedule, work list, and parts list. The output of the ERM to the Supervisory Control is likely a series of operational options with a PRA-based success probability for each. We

anticipate that the ERM will generate a predictive output that quantifies the potential change in risk for a reduction in power (or other maneuver) in order to increase the success probability of avoiding an unplanned outage or decrease in safety margins.

The supervisory control logic may utilize additional information (such as diagnostic information from the ECA) in its decision making process. In addition, prognostic information that indicates the rate of degradation of SSC may be needed by the supervisory control algorithms to indicate an automatic trip of equipment that is suffering fast degradation (though this may be better handled by trip devices on SSC).

4.3 Some Observations

Given the likely needs from the Supervisory Control algorithms, and the potential outputs available from the ERM, the following observations may be made:

- The supervisory control logic needs to support operational modes that reduce demands on SSC experiencing degraded condition, at least until the next available opportunity for maintenance and return to serviceable condition. Note that this will require the ERM to provide information that enables the appropriate tradeoffs (revenue generated by running the plant in a degraded state vs. incremental risk in terms of cost and safety metrics). Ideally, the operation of the plant can be extended to the next maintenance outage. However, if there is no option that will make it to the next planned outage (above some predefined minimum success probability), then other time periods will need to be considered. A useful practical minimum for remaining run time might be to run long enough to obtain parts and materials for repair.
- The ERM needs to provide output periodically (say hourly or daily) to the Supervisory Control during steady state, as well as “on demand” when plant power or power split (electrical to thermal) changes by some threshold amount. On demand output should also be provided when significant SSC is diagnosed with a problem.
- Any ERM output that triggers action by the Supervisory Control modules needs to be available to the (human) operator for review in an easy to comprehend format.
- Ideally, the ERM and/or the PSM needs to evaluate not only success probability of operating particular SSC until the next scheduled outage, but also (if possible) to calculate the probability of doing more expensive to repair damage to SSC by continuing to run them. This is effectively a cost-benefit analysis. For example, minor failure of a bearing can frequently be repaired by just replacing the bearing material itself, without having to rework the shaft. Continued operation at loose clearances can damage the shaft itself, considerably complicating repair and ratcheting cost upwards.
- A mechanism for self-test or test by the Supervisory Control Module might be useful to verify that the ERM module(s) are operating properly, and are not suggesting counterproductive or unnecessary action.

These observations may lead to substantial computational complexity of both the supervisory control and ERM modules. To reduce the computational demand on the overall system (supervisory control and ERM):

- It may be useful to limit the number of power reduction options to limit the number of choices the Supervisory Control has to make. An example may be options that reduce the power output in integral multiples of 5% (95%, 90%, 85% etc.), at least initially. This is to simplify the needed ERM calculations to account for the opportunity cost of operating the plant for an extended period of time below 100% power. Note that the cost of running the plant for a fixed period of time is (roughly) the same regardless of plant power, while generation revenue is proportional to plant power.
- It may be useful to suppress operational options with success probabilities below some threshold, to help focus the supervisory control algorithm to only viable options. Determination of the minimum viable success probability will need to be done carefully, and would involve an assessment of the various possible risk metrics to better understand the tradeoffs involved.

5.0 Summary

Enhanced risk monitors that integrate ECA and prognostics information to calculate time- and condition-dependent failure probabilities have the potential to enable real-time decisions about stress relief for susceptible equipment while supporting effective maintenance planning. As a result, ERMs are expected to improve the safety, availability, and affordability of AdvSMRs.

An initial methodology for integrating time-dependent failure probabilities into risk monitors was developed. The methodology was evaluated using a hypothetical PRA model from a simplified model of a liquid-metal-cooled AdvSMR. Component failure data from industry compilation of failures of components similar to those in the simplified AdvSMR model were used to initialize the PRA model. By using time-dependent probability of failure that grows from the initial probability when equipment is in like-new condition to a maximum probability of failure, which occurs before a scheduled maintenance action that restores or repairs the component to "as-new" condition, we computed and analyzed the changes in CDF over time.

The results indicate that, using the proposed methodology for ERM, as the failure probabilities and failure rates change over time, the CDF changes over time. Repairs or replacements (bringing the components to as-new condition) reduce the risk, although aging of other components may still drive the overall risk higher.

Uncertainty analysis indicated that the ability to propagate uncertainties in various inputs to the ERM provides useful information. Specifically, the uncertainty bounds in the ERM output can have an impact on the ability to perform quantitative assessments of the changes in O&M and safety risk metrics due to component degradation. Improved quantification of the sources of uncertainty will be needed to improve the ability to perform these kinds of trade-off analyses.

In addition, we initiated a study on alternative risk metrics for AdvSMRs. Several possible options for alternative risk metrics were identified and need further evaluation to determine their overall benefit to the AdvSMR program.

5.1 Ongoing and Planned Future Research

Ongoing and planned research is focused on evaluating alternative risk metrics (including the options described earlier) and the impact of uncertainty on these risk metrics. In addition, we anticipate integrating the ERM methodology with simulation tools that simulate advanced reactor/AdvSMR modules and the impact of component degradation on their performance to perform comprehensive evaluations of the ERM methodology. In addition, we will explore the possibility of evaluations using experimental data, and to this end, will continue to evaluate sources of relevant reliability data, including data from test reactors, and available test-beds.

Currently, the traditional risk measure of core damage frequency is being used for initial framework development and testing; however, future work will investigate non-safety-related risk measures, such as economic risk. Additional evaluations of the postulated importance measure are also needed. In addition, alternative importance measures that can provide diagnostic information that can be valuable in informing equipment-related planning and maintenance activities are also needed.

6.0 References

Abram T and S Ion. 2008. "Generation-IV Nuclear Power: A Review of the State of the Science." *Energy Policy* 36(12):4323-4330.

Anheier NC, JD Suter, HA Qiao, ES Andersen, EJ Berglin, M Bliss, BD Cannon, R Devanathan, A Mendoza and DM Sheen. 2013. *Technical Readiness and Gaps Analysis of Commercial Optical Materials and Measurement Systems for Advanced Small Modular Reactors* SMR/ICHMI/PNNL/TR-2013/04; PNNL-22622, Rev. 1, Pacific Northwest National Laboratory, Richland, Washington.

Apostolakis G. 2000. "The Nuclear News Interview—Apostolakis: On PRA." *Nuclear News* 43(3):27-31.

Arjas E and J Holmberg. 1995. "Marked Point Process Framework for Living Probabilistic Safety Assessment and Risk Follow-up." *Reliability Engineering & System Safety* 49(1):59-73.

Cetiner SM, DG Cole, DL Fugate, RA Kisner, MA Kristufek, AM Melin, MD Muhlheim, NS Rao and RT Wood. 2013. *Definition of Architectural Structure for Supervisory Control System of Advanced Small Modular Reactors*. SMR/ICHMI/ORNL/TR-2013/04, Oak Ridge National Laboratory, Oak Ridge, Tennessee.

Coble JB, GA Coles, P Ramuhalli, RM Meyer, EJ Berglin, DW Wootan and MR Mitchell. 2013. *Technical Needs for Enhancing Risk Monitors with Equipment Condition Assessment for Advanced Small Modular Reactors*. PNNL-22377 Rev. 0; SMR/ICHMI/PNNL/TR-2013/02, Pacific Northwest National Laboratory, Richland, Washington.

David PA, R Maude-Griffin and G Rothwell. 1996. "Learning by Accident? Reductions in the Risk of Unplanned Outages in U.S. Nuclear Power Plants after Three Mile Island." *Journal of Risk and Uncertainty* 13(2):175-198.

Daw J, J Rempe, P Ramuhalli, R Montgomery, HT Chien, B Tittmann and B Reinhardt. 2012. *NEET In-Pile Ultrasonic Sensor Enablement-FY 2012 Status Report*. INL/EXT-12-27233, PNNL-21835, Idaho National Laboratory, Idaho Falls, Idaho.

Eide SA, TE Wierman, CD Gentillon, DM Rasmussen and CL Atwood. 2007. *Industry-Average Performance for Components and Initiating Events at U.S. Commercial Nuclear Power Plants*. NUREG/CR-6928, INL/EXT-06-11119, U.S. Nuclear Regulatory Commission, Washignton, D.C.

EPRI. 2011. "Basics of Nuclear Power Plant Probabilistic Risk Assessment." Electric Power Research Institute (EPRI), Palo Alto, California. Presented at Fire PRA Workshop 2011 in San Diego, California, and Jacksonville, Florida.

EPRI. 2013. "Computer Aided Fault Tree System (CAFTA), Version 6.0 Demo." Electric Power Research Institute, Palo Alto, California. http://www.epri.com/abstracts/Pages/ProductAbstract.aspx?ProductId=000000000001015514.

Fulwood RR and RE Hall. 1988. *Probabilistic Risk Assessment in the Nuclear Power Industry: Fundamentals and Applications*. Pergamon Press. ISBN 0080363628.

Haasl D, J Young and W Cramond. 1988. *Probabilistic Risk Assessment Course Documentation*. NUREG/CR-4350, U.S. Nuclear Regulatory Commission, Washington, D.C.

IAEA. 2002. *Nuclear Power Plant Outage Optimisation Strategy*. IAEA-TECDOC-1315, International Atomic Energy Agency, Vienna, Austria.

IAEA. 2006. *Management Strategies for Nuclear Power Plant Outages*. Technical Report Series No. 449, International Atomic Energy Agency, Vienna, Austria.

Kafka P. 2008. "Probabilistic Risk Assessment for Nuclear Power Plants." In *Handbook of Performability Engineering*, pp. 1179-1192, Ch. 71. ed: KB Misra. Springer, London.

Kidd S. 2011. "Nuclear Power Plants -- How Have They Become Like ATMs?" *Nuclear Engineering International*. Available at http://www.neimagazine.com/opinion/opinionnuclear-power-plants-how-have-they-become-like-atms/.

Marshall FM, DM Rasmuson and A Mosleh. 2007. *Common-Cause Failure Parameter Estimations*. NUREG/CR-5497, INEEL/EXT-97-01328, U.S. Nuclear Regulatory Commission, Washington, D.C.

Meyer RM, JB Coble, EH Hirt, P Ramuhalli, MR Mitchell, DW Wootan, EJ Berglin, LJ Bond and CH Henager Jr. 2013a. *Technical Needs for Prototypic Prognostic Technique Demonstration for Advanced Small Modular Reactor Passive Components*. PNNL-22488 Rev. 0, SMR/ICHMI/PNNL/TR-2013/01, Pacific Northwest National Laboratory, Richland, Washington.

Meyer RM, P Ramuhalli, EH Hirt, AF Pardini, AM Jones, JE Deibler, SG Pitman, JC Tucker, M Prowant and JD Suter. 2013b. *Prototypic Prognostics Health Management Systems for Passive AdvSMR Components*. PNNL-22889 Rev. 0, SMR/ICHMI/PNNL/TR-2013/06, Pacific Northwest National Laboratory, Richland, Washington.

Miller JS, B Stakenborghs and R Tsai. 2011. "Improving Nuclear Power Plant's Operational Efficiencies in the USA." In *19th International Conference on Nuclear Engineering (ICONE19)*. May 16-19, 2011, Makuhari, Japan. American Society of Mechanical Engineers, New York. Paper ICONE19-43791.

Nagatomi Y, Y Matsuo and T Murakami. 2010. "U.S., European and South Korean Efforts to Raise Nuclear Power Plant Utility factors - What Japan Should Learn from These Efforts." *The Institute of Energy Economics, Japan Energy Journal*. Available at https://eneken.ieej.or.jp/data/3285.pdf.

NEI. 2014. *U.S. Nuclear Refueling Outage Days*. Nuclear Energy Institute (NEI). Washington, D.C. Accessed June 10, 2014. Available at http://www.nei.org/Knowledge-Center/Nuclear-Statistics/US-Nuclear-Power-Plants/US-Nuclear-Refueling-Outage-Days.

NRC. 2012. *Probabilistic Risk Assessment (PRA)*. U.S. Nuclear Regulatory Commission (NRC). Washington, D.C. Accessed October 17, 2012. Available at http://www.nrc.gov/about-nrc/regulatory/risk-informed/pra.html (last updated March 29, 2012).

NRC. Undated. "Tutorial on Probabilistic Risk Assessment (PRA)." U.S. Nuclear Regulatory Commission (NRC), Washington, D.C. http://www.nrc.gov/about-nrc/regulatory/risk-informed/rpp/pra-tutorial.pdf.

OECD. 2000. *Status Report on Nuclear Power Plant Life Management*. NEA/SEN/NDC(2000)6, Organisation for Economic Co-operation and Development/Nuclear Energy Agency/Nuclear Development Committee, Paris, France.

Papazoglou IA. 1998. "Mathematical Foundations of Event Trees." *Reliability Engineering and System Safety* 61(3):169-183.

Puglia WJ and B Atefi. 1995. "Examination of Issues Related to the Development and Implementation of Real-Time Operational Safety Monitoring Tools in the Nuclear Power Industry." *Reliability Engineering and System Safety* 49(2):189-199.

Ramuhalli P, GA Coles, JB Coble and EH Hirt. 2013. *Technical Report on Preliminary Methodology for Enhancing Risk Monitors with Integrated Equipment Condition Assessment*. PNNL-22752, Rev. 0; SMR/ICHMI/PNNL/TR-2013/05, Pacific Northwest National Laboratory, Richland, Washington.

Ramuhalli P, JW Griffin, JM Fricke and LJ Bond. 2012. "An Assessment of Uncertainty in Remaining Life Estimation for Nuclear Structural Materials." In *8th International Topical Meeting on Nuclear Plant Instrumentation, Control and Human Machine Interface Technologies (NPIC&HMIT 2012)*, pp. 1325-1337. July 22-26, 2012, San Diego, California. American Nuclear Society, La Grange Park, Illinois.

Smith CL, VN Shah, T Kao and GE Apostolakis. 2001. *Incorporating Aging Effects into Probabilistic Risk Assessment - A Feasibility Study Utilizing Reliability Physics Models*. NUREG/CR-5632, U.S. Nuclear Regulatory Commission, Washington, D.C.

Vesely W, F Goldberg, N Roberts and D Haasl. 1981. *Fault Tree Handbook*. NUREG-0492, U.S. Nuclear Regulatory Commission, Washington, D.C.

Vesely WE, TC Davis, RS Denning and N Saltos. 1983. *Measures of Risk Importance and Their Applications*. NUREG/CR-3385, BMI-2103, U.S. Nuclear Regulatory Commission, Washington, D.C.

Vesely WE and AJ Wolford. 1988. "Risk Evaluations of Aging Phenomena: The Linear Aging Reliability Model and Its Extensions." *Nuclear Engineering and Design* 108:179-185.

Wu JS and GE Apostolakis. 1992. "Experience with Probabilistic Risk Assessment in the Nuclear Power Industry." *Journal of Hazardous Materials* 29(3):313-345.

Yoshikawa H, M Yang, M Hashim, M Lind and Z Zhang. 2011. "Design of Risk Monitor for Nuclear Reactor Plants." *Nuclear Safety and Simulation* 2(3):266-274.

Appendix A

Generic AdvSMR PRA Model Description

Appendix A

Generic AdvSMR PRA Model Description

A.1 Probabilistic Risk Assessment

In general, risk can be defined as the product of the frequency of an event and its consequence:

$$Risk = Frequency \times Consequence$$

where *Consequence* refers to undesirable outcomes (reactor core damage, release frequency of radionuclides, cancer deaths, etc.) and *Frequency* is the likelihood of the consequence per unit time. In the nuclear industry, risk is typically evaluated for events that have consequences related to public health and safety.

The assessment of risk with respect to NPPs is intended to achieve the following general objectives (Fulwood and Hall 1988):

- Identify initiating events and event sequences that might contribute significantly to risk;
- Provide realistic quantitative measures of the likelihood of the risk contributors;
- Provide a realistic evaluation of the potential consequences associated with hypothetical accidents; and
- Provide a reasonable risk-based framework for making decisions regarding nuclear plant design, operation, and siting.

PRA is a systematic safety analysis methodology that (Haasl et al. 1988; Apostolakis 2000) begins by identifying undesirable consequences (e.g., reactor unavailability, core damage, release of radioactivity) and initiating events that can lead to these consequences. This is followed by systematically identifying accident sequences [defined by event trees (Papazoglou 1998) and fault trees (Vesely et al. 1981)] through which the facility can move from the initiating event to the undesired consequence. The PRA model then calculates the probability of occurrence for each accident sequence and ranks the accident sequences according to probability of occurrence (or, alternatively, contribution to the undesirable event) to manage the major contributors to risk.

Three levels of PRA, designated by the type of risk being assessed, have been considered for NPPs (NRC 2012). Level 1 PRA estimates the frequency of accidents that cause core damage (commonly called core damage frequency); Level 2 PRA, the frequency of radioactive release from the NPP (assuming that the core is damaged); and Level 3, the consequences to the public and environment outside the NPP from Level 2 radioactive releases. The ultimate result of the PRA is the probability of each undesirable consequence (e.g., core damage, radioactive release) and a list of the major contributors to its occurrence.

A full PRA model consists primarily of event trees and fault tree models that, when solved, produce cutsets representing the combinations of failures that result in an accident sequence and define the

likelihood of those failures (EPRI 2011). Fault trees and event trees define Boolean relationships among fault events that cause the top event to occur. Event trees define logic among fault trees in a way that accident sequences can be translated entirely into an equivalent set of Boolean equations. This logic can be reduced to an expression of cutsets. The list of cutsets for an accident sequence represents all combination failures leading to that accident sequence. The dominant cutsets represent the most important combinations along with the frequency or probability of those failures.

An event tree is a diagram that defines accident sequences. Each horizontal "pathway" running from left to right through an event tree defines an accident sequence beginning with an initiating event, followed by a series of top events (i.e., the systems and/or actions needed to mitigate the initiating event), and finishing at a particular plant end state (e.g., plant damage). Each branch point of the event tree represents a question asked about the status or condition of a system. Traditionally, the up branches indicate success while the down branches indicate failure. Figure A.1 shows an example event tree.

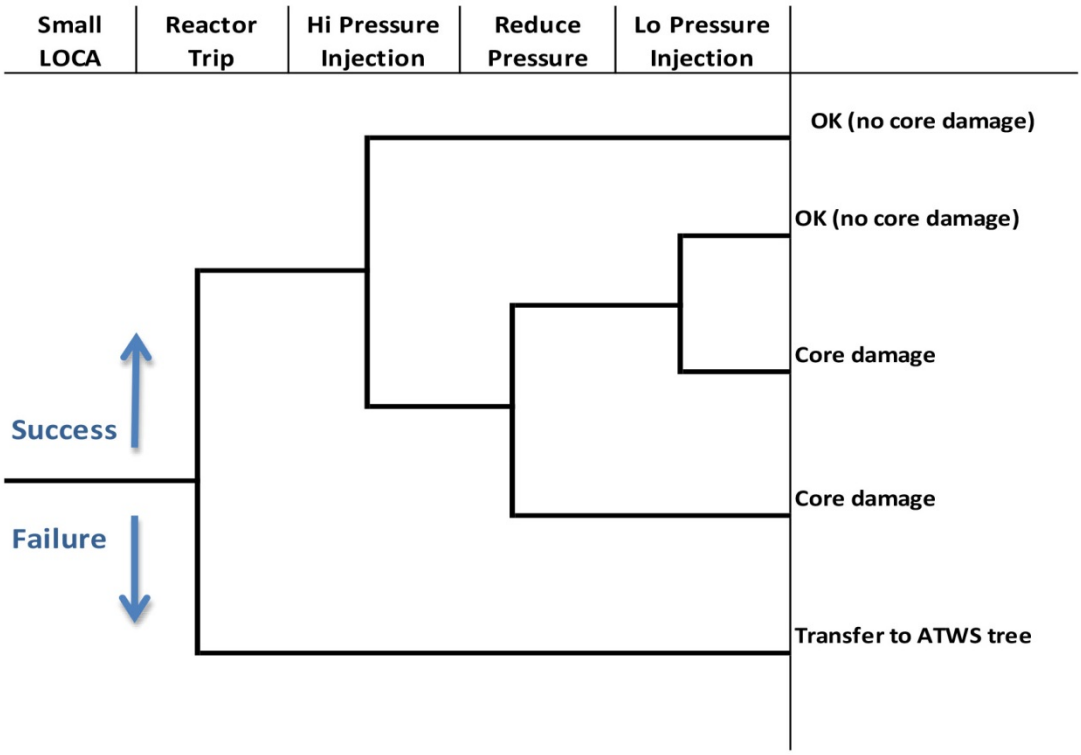

Figure A.1. Simplified Reactor PRA Event (NRC Undated)

Fault trees are graphic models depicting the various fault combinations that will result in the occurrence of an undesired (i.e., top) event. A simple fault tree is presented in Figure A.2. Fault tree analysis is an analytical technique, whereby an undesired state of the system is specified, and the system is analyzed in the context of its environment and operation to find all credible ways in which the undesired event can occur (Vesely et al. 1981).

Both passive and active components may be included in fault trees and event trees. Typical active component failures include: 1) failure to run, 2) failure to start, 3) failure to open or close or operate, and

4) unavailability because of test or maintenance. Typical passive component failures include: 1) rupture, 2) plugging, 3) failure to remain open or closed, and 4) cold or hot short of power or instrument cables.

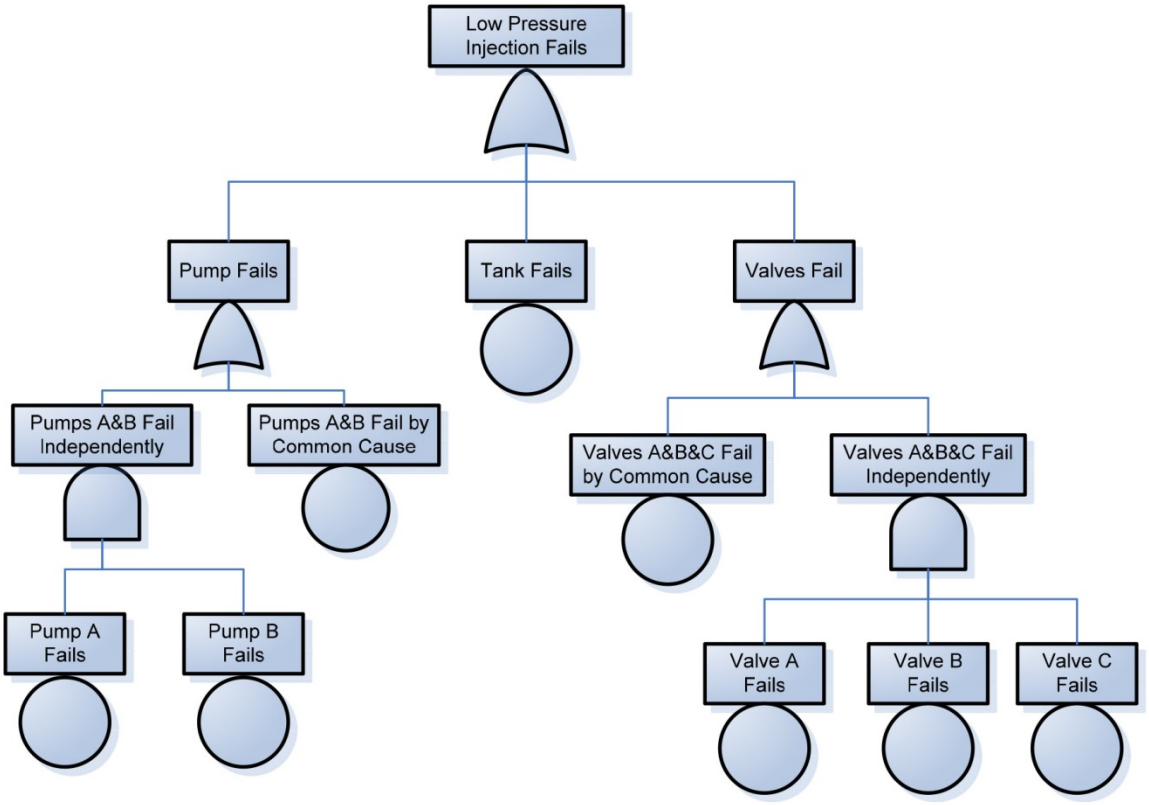

Figure A.2. Simplified Example Fault Tree (NRC Undated)

Each failure event in the fault tree is called a basic event and has a component failure or human error probability associated with it. Component failures are typically demand- or time-related (e.g., valve fails to close on demand, or pump fails to run for 24 hours). Data for component failure rates and failure probabilities comes from generic sources, plant-specific sources, or a combination of the two (as when generic data is adjusted using plant-specific data by performing a Bayesian update). Aging-related failure data, if included, typically utilizes reliability models (Vesely and Wolford 1988; Smith et al. 2001). Human error probabilities are generally compiled using human reliability analysis (HRA) that is based on research done in NPP control rooms and simulators. HRA is an important part of PRA, and considers such performance-shaping factors as stress level, crew resources, cues, and timing.

Importance analysis is typically performed on the results of a PRA and provides a quantitative perspective on risk and sensitivity of risk to changes in input values (Vesely et al. 1983). Three commonly encountered importance analyses are determination of risk achievement worth (RAW), risk reduction worth (RRW), and Fussell-Vesely (F-V). These analyses produce different kinds of measures of basic or initiating event importance, such as determining the ratio of the total CDF produced when a particular basic event is set to either one or zero to the baseline CDF produced when the basic or initiating event is set to its nominal value. For instance, RRW analysis uses the ratio of the baseline risk to the

reduced risk calculated by assuming a component is completely reliable (i.e., no failures) (Vesely et al. 1983). Importance measures are valuable in sorting out the most important component failure modes.

Uncertainty in PRA modeling arises from a number of sources that are typically divided into aleatory variability and epistemic uncertainty (EPRI 2011). Aleatory variability is related to the statistical confidence we have in failure probability data, while epistemic uncertainty is related to the uncertainty in the accident sequences used to develop the PRA model. Epistemic uncertainty is dealt with by developing event and fault trees as complete as possible, identifying keys sources of uncertainty, and performing sensitivity analyses. The aleatory variability is addressed explicitly by propagation of parametric data uncertainty for initiating basic event data. Uncertainty analysis is performed through a sampling strategy (e.g., Monte Carlo sampling) over some number of observations.

As PRA models are integrated into plant management, they have become living models that reflect the as-modified and as-operated plant configuration and are able to estimate the changing likelihood of undesired events. Risk monitors extend the PRA framework by incorporating the actual and dynamic plant configuration (e.g., equipment availability, operating regimes, and environmental conditions) into the risk assessment, although failure data on equipment is based on operational experience and reliability analysis, and unit-specific failure information is generally not used.

A.2 Simplified-Model AdvSMR Design

As described in Section 2.4.2, a simplified-model AdvSMR (power block) design is used in the development of the PRA model used for the research that supported the development of a framework for ERMs. This simplified model is shown in Figure A.3. This hypothetical design is intended to be prototypical and resembles proposed liquid metal-cooled SMR designs. The example design is defined to provide a simple level of abstraction but contains enough resolution and specific design elements to inform the development of a PRA model that, when quantified, produces a cogent set of results.

The simplified-model AdvSMR design in Figure A.3 is a small, modular, pool-type, liquid-metal-cooled reactor assumed to be producing 200 to 500 MWt[(1)] of power. The plant design consists of an unspecified number of identical power blocks, with each power block comprised of two reactor modules. Each module is connected to its own intermediate heat exchange system and steam generator. The secondary side (i.e., steam side) equipment is located in a different building and connects two modules to form a power block. A power block feeds a single variable capacity turbine generator. (*Note: While a greater number of reactor modules in a power block are possible, two modules provide sufficient complexity to develop and demonstrate a methodology for ERM.*)

(1) The electrical output of a reactor depends on the efficiency of the power conversion process.

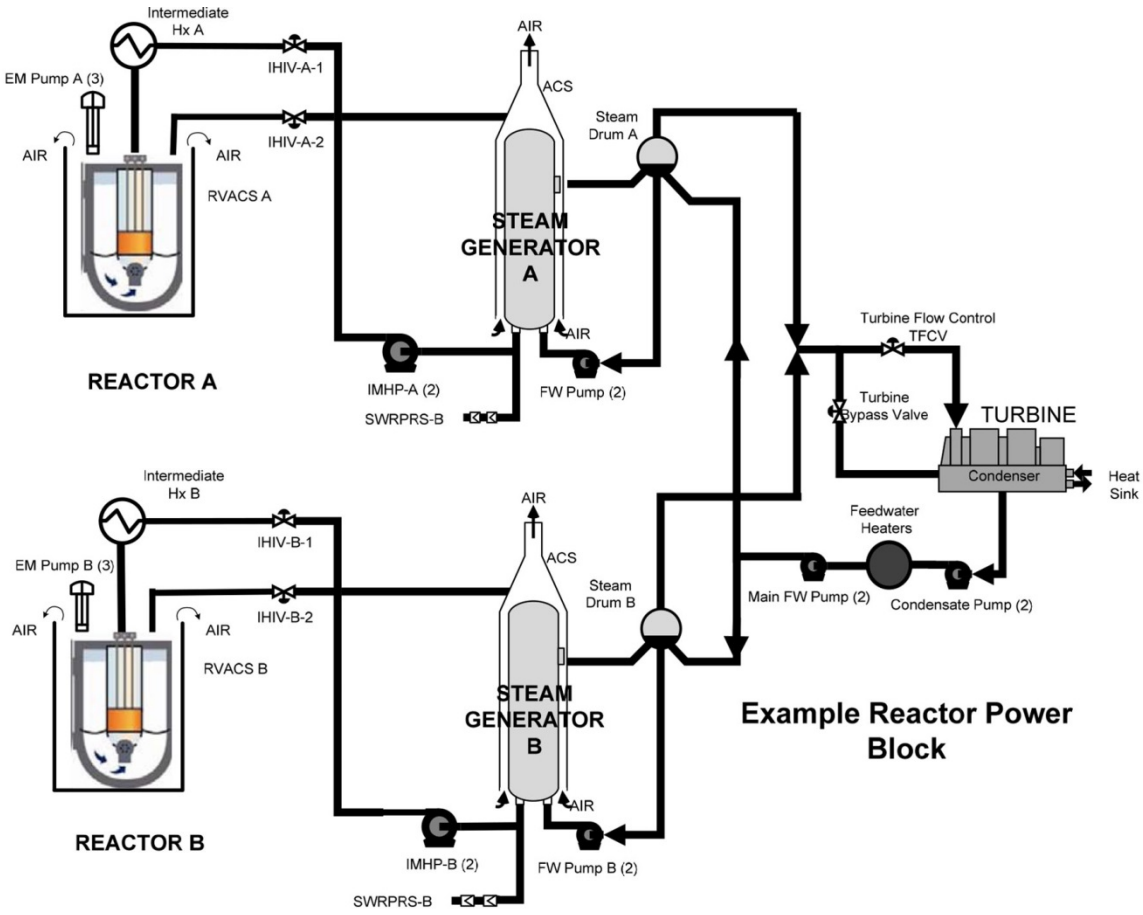

Figure A.3. One-Line Diagram of Simplified-Model AdvSMR

A.2.1 Key Components in the Simplified-Model AdvSMR Design

The components defined for modeling in the example reactor power block are:

- Electromagnetic pumps (3 per reactor module)
- RVACS (1 per reactor module)
- Intermediate heat exchangers (1 per reactor module)
- Intermediate loop isolation valves (2 per reactor module)
- Intermediate loop pumps (2 per reactor module)
- Steam generators (1 per reactor module)
- SWRPRS (1 per reactor module)
- Steam drum (1 per reactor module)
- Feedwater pumps (2 per reactor module)
- Passive steam generator cooling system (1 per reactor module)

- Turbine generator (1 per power block)
- Turbine bypass valve (1 per power block)
- Turbine flow control valve (1 per power block)
- Main feedwater pumps (2 per power block)
- Main feedwater heater (1 per power block)
- Main condensate pumps (2 per power block)
- Emergency diesel generator (1 per power block)

The primary features of the simplified design are the primary cooling loop, intermediate cooling loop, secondary system including the steam generators, and residual heat removal systems consisting of a passive RVACS and passive steam generator cooling system.

The primary loop is contained entirely within the reactor vessel. Liquid sodium is pumped by electromagnetic pumps up through the reactor core and out through the top. Flow is then forced back down through the space (annulus) between the outer wall and reactor core past two intermediate heat exchangers. The electromagnetic pumps are suspended into the reactor pool from above. Because electromagnetic pumps have no moving parts and therefore there is no associated "flywheel effect," a synchronous coast-down function is designed into pumps to provide coast-down upon loss of power.

The intermediate loop transfers heat to the secondary system via two steam generators. The primary components of this system are the steam generator, the intermediate cooling pumps, and the intermediate loop isolation valves. The intermediate cooling pumps force flow of heated liquid sodium from the intermediate heat exchangers to the steam generators during both normal and upset conditions. The isolation valves close to isolate the reactor from a pressure increase resulting from a sodium-water interaction that would occur in the event of a steam generator tube rupture event. The signal to close these isolation valves is based on opening of passive pressure relief valves connected directly to the steam generators. Together the isolation and pressure relief valves constitute part of the SWRPRS.

The secondary system consists of a steam generator and a steam drum for each reactor module connected to a single turbine generator. The secondary system delivers steam from the steam generators to the inlet of the turbine. Turbine steam exhaust flows through the condensers and then to main condensers and feedwater pumps back to the reactor module steam drums where it can be pumped by the reactor module feedwater to the steam generators. The turbine bypass valves allow steam to flow past the turbine and directly into the condenser when required. This allows a means of residual heat removal from the reactor modules during reactor shutdown and startup, and provides a flow path that will be needed in case of load rejection and some event that trips the turbine. Each steam generator has a sodium-water reaction pressure-relief system that relieves pressure in the event of a generator tube rupture. This is a passive system and provides a path for the increased steam pressure that would occur from sodium-water reaction.

The residual heat removal system consists of RVACS and the passive steam generator cooling system. The passive steam generator cooling system removes heat by air circulation past the steam generators. This airflow is initiated by remote manual opening of louvers at the inlet and outlet of the shroud around the steam generators. In this mode, heat is removed by natural convection to the air. This

system can operate with forces or natural circulation of intermediate cooling loop sodium. If operators are unsuccessful at opening louvers to initiate convective cooling or if the intermediate cooling flow or inventory is lost, then residual heat can by removed by natural air circulation around the containment vessel that surrounds the reactor vessel via the RVACS. Heat will be transferred from the reactor vessel to the containment vessel by radiative heat transfer and then to the air around the containment vessel and ultimately the atmosphere via convective heat transfer. A key design feature of RVACS is that no components or operator actions are required to initiate RVACS, because it is continually operating during normal power operation and is designed to be able to accommodate residual heat transfer after reactor shutdown.

A.3 PRA for Simplified-Model AdvSMR

The PRA model developed for the simplified-model AdvSMR is capable of modeling fault (or accident) sequences that could occur, induced by a perturbation (or initiating event) in the system, and of identifying the combinations of system failures, support system failures and human errors that could lead to core damage. The general framework for the PRA model discussed herein includes the following analyses, each of which are discussed in detail below:

- Initiating Event Analysis
- Accident Sequence Analysis
- Systems Analysis
- Data Analysis
- Common Human Reliability Analysis
- Cause Failure Analysis
- Quantification

A.3.1 Initiating Event Analysis

An initiating event is an event that could lead directly to core damage (e.g., reactor vessel rupture) or that challenges normal operation and requires successful mitigation using safety or non-safety systems to prevent core damage. Identifying initiating events is the first step in the development of plant accident sequences, which are discussed further in Section A.3.2. The identification of initiating events applicable to a plant system is an iterative process that requires feedback from other PRA elements, such as system analysis, and review of plant or generic industry experience/data. The initiating events considered for the simplified-model AdvSMR are outlined in Table A.1.

Table A.1. Initiating Events for Simplified-Model AdvSMR

Loss of Electromagnetic Pump	Loss of Main Feedwater Pump
Loss of Feedwater Pump	Reactor Transient (Trip)
Loss of Intermediate Loop Pump	Plug or Failure of RVACS due to External Event
Intermediate Heat Exchanger Tube Rupture	Steam Generator Tube Rupture
Loss of Offsite Power	Anticipated Transient Without SCRAM
Loss of Main Condensate Pump	Loss of Main Feedwater Pump

A.3.2 Accident Sequence Analysis

Conceptually, each accident sequence can be thought of as a combination of an initiating event, which triggers a series of plant system and/or operator responses, with a certain combination of successes and/or failures of these responses that leads to a core damage state. The fault tree linking approach, which involves a combination of event trees and fault trees, was used to identify and analyze the plant functions required to respond to each identified initiating event to prevent core damage. Event trees are developed to outline the broad characteristics of the accident sequences that start from the initiating event and, depending on the success or failure of each defined plant function, lead to a successful outcome or to damage to a core damage event. Fault trees are then used to model the failure of the key and supporting systems that are deemed necessary to carry out each plant function. Initiating events that require the same or similar plant response may be grouped into categories that each uses a single event tree. The resulting event tree for simplified-model AdvSMR is presented in Figure A.4.

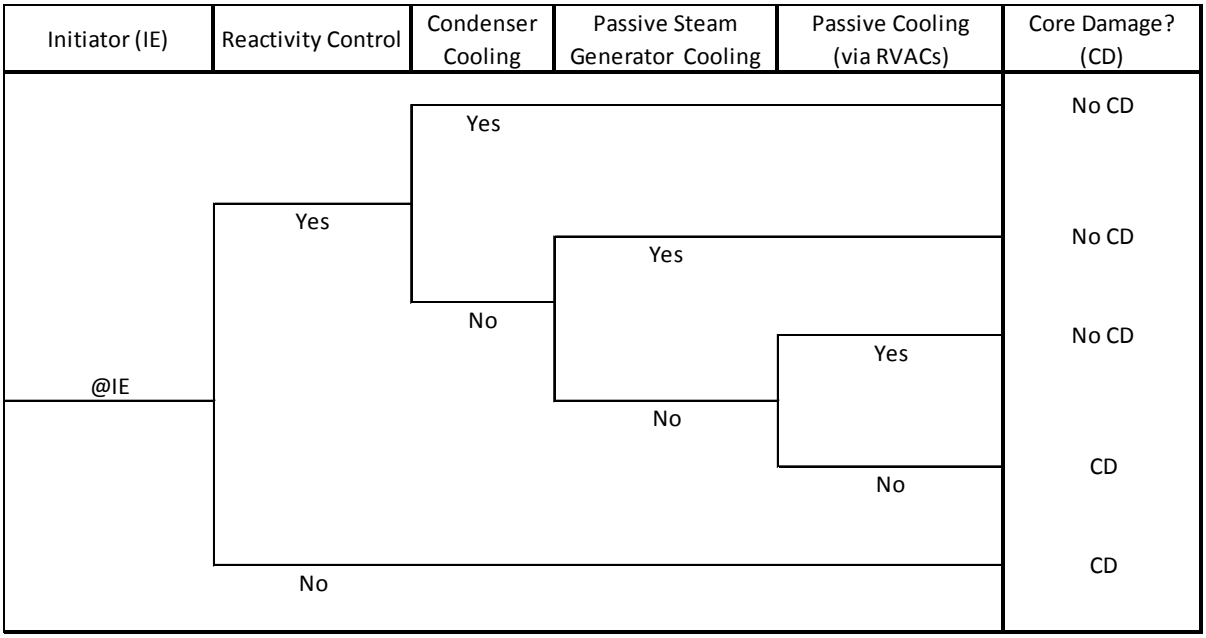

Figure A.4. Event Tree for Simplified-Model AdvSMR

A.3.3 Systems Analysis

To model the system failures that are identified in the accident sequence analysis outlined in Section A.3.2, a system analysis is performed on each key and supporting system deemed necessary to carry out the functions delineated in the event tree. This is done by means of fault tree analysis, which extends down to the level of individual basic events that include component failures (e.g., failures of pumps, valves, diesel generators, etc.), unavailability of components during periods of maintenance or testing, common cause failures of redundant components and human failure events that represent the impact of human errors.

The overall mission time assumed by the PRA model is 24 hours. The mission times assumed for each component and/or system vary according to characteristics of available failure data as well as the time period over which each plant function is defined. The failure criteria for each key and supporting system are represented by the logical inverse of the accident sequence success criteria. Table A.2 presents the assumptions implicit to the success criteria defined for key systems modeled within the PRA developed for the simplified-model AdvSMR; each system is also cross-referenced to the plant functions defined in Figure A.4.

Table A.2. Success Criteria for the Simplified-Model AdvSMR PRA Model

Key System	Description of System Failure	Success Criteria	Plant Function Supported
RSS/RPP	The reactor shutdown or protection system (RSS/RPP) fails to trip the reactor and maintain reactivity control.	Four out of six control rod units, one out of four trip sensors, one out of four SCRAM breakers, and accurate trip setpoints are required for each module.	Reactivity Control
TB	The turbine bypass (TB) system fails to allow steam to flow past the turbine and directly into the condenser when required (e.g., in case of load rejection and some event that trips the turbine).	The turbine bypass valve is required to open for one or two modules.	Condenser Cooling
MFW	The main feedwater (MFW) system fails to provide feedwater to module steam drums to establish decay heat removal via the condenser.	One out of two MFW pumps is required for one or two modules. Both pumps are assumed to be running.	Condenser Cooling
FW	The feedwater (FW) system fails to provide feedwater to module steam generators to establish decay heat removal via the condenser.	One out of two module feedwater pumps is required for each module. Both pumps are assumed to be running.	Condenser Cooling
CD	The condensate (CD) system fails to remove decay heat via the condenser.	One out of two main condensate pumps is required for one or two modules. Both pumps are assumed to be running.	Condenser Cooling

Key System	Description of System Failure	Success Criteria	Plant Function Supported
PTHS	The primary heat transport system (PHTS) fails to maintain flow of sodium through the reactor vessel and consequently remove decay heat via the intermediate heat exchangers.	One out of three electromagnetic pumps is required for each module. Two pumps are assumed to be running, and one is assumed to be in standby.	Condenser and Passive Steam Generator Cooling
ITHS	The intermediate heat transport system (IHTS) fails to transfer heat via the intermediate heat exchangers to the secondary system for decay heat removal through the steam generator.	One out of two intermediate loop pumps is required for each module. Two are required in case of an intermediate heat exchanger tube rupture. Both pumps are assumed to be running.	Condenser and Passive Steam Generator Cooling
Passive Steam Generator Cooling	The passive steam generator cooling system fails to remove heat by air circulation past the steam generators. This airflow is initiated by remote manual opening of louvers (SGLs) at the inlet and outlet of the shroud around the steam generators. In this mode, heat is removed by natural convection to the air.	The SGLs are required to open for each module.	Passive Steam Generator Cooling
SWRPRS	The SWRPRS fails to isolate a SGTR-initiated sodium-water reaction that subsequently fails the IHTS and PHTS by means of an unrecoverable loss of sodium.	In case of a steam generator tube rupture, either both the intermediate loop isolation valves or the SWRPRS is required to prevent a loss of coolant accident from the reactor vessel, which would make RVACs ineffective.	Passive Cooling
RVACS	Residual heat cannot be removed by natural air circulation around the containment vessel that surrounds the reactor vessel via the RVACS.	Sufficient heat (i.e., to prevent core damage) must be transferred from the reactor vessel to the containment vessel by radiative heat transfer and then to the air around the containment vessel and ultimately the atmosphere via convective heat transfer. For failure of RVACS caused by external events such as high winds, the opportunity for recovery (e.g., unplug radiating fins) by plant operators was assumed to be possible.	Passive Cooling

For key systems with more than one train (or additional form of redundancy) available, the PRA model uses a nomenclature that assigns a module identifier (i.e., A or B) as well as a train identifier (i.e., 1, 2 or 3, as applicable) to each component. The system analysis performed on support systems and the resulting success criteria are limited to power dependencies modeled within the PRA according to the simplified electrical arrangement presented in Figure A.5. For key systems with single level of redundancy, each train is assumed to be dependent on a single electrical division (i.e., Division A or B) for power, whereas for those systems with an additional layer of redundancy, the third train may be fed from either electrical division. Two standby emergency diesel generators are assumed for the power

block; however, one is assumed to be sufficient for required shutdown loads. A typical fault tree logic model that results from the system analysis, in this case for the three electromagnetic pumps that support the primary heat transport system, is shown in Figure A.6.

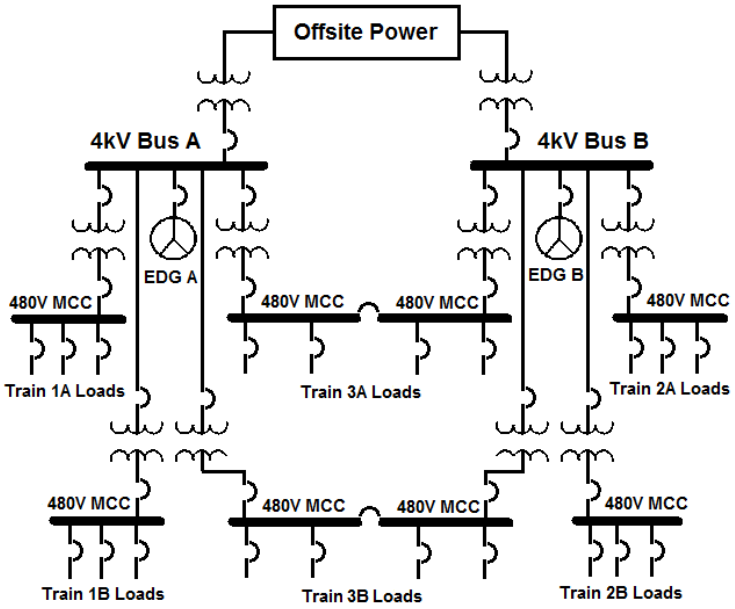

Figure A.5. Simplified One-Line Diagram of Electrical System

A.3.4 Data Analysis

Table A.3 presents the initiating event and system component failure probabilities used within the baseline PRA for the simplified-model AdvSMR (i.e., the failure probabilities when the components are as-built). Note that some components in this listing actually represent system-level failures, such as RVACS. Supporting systems, such as electrical power systems, instrumentation, and the reactor trip system, are also reflected in this list.

For this analysis, where available, industry documented failure data (Eide et al. 2007) was used to define initiating event and component failure likelihoods for the key components in the simplified-model AdvSMR design. Note, however, that some latitude was taken in adjusting these values for the simplified-model AdvSMR design, specifically for components where such data is not readily available. In these cases, assumed failure data was based on available operational experience and like-kind components.

Unavailability of components during periods of maintenance or testing was assumed to occur at intervals of 0.5, 1, and 3 weeks per year, based on the risk significance of the component and level of system and/or functional redundancy available.

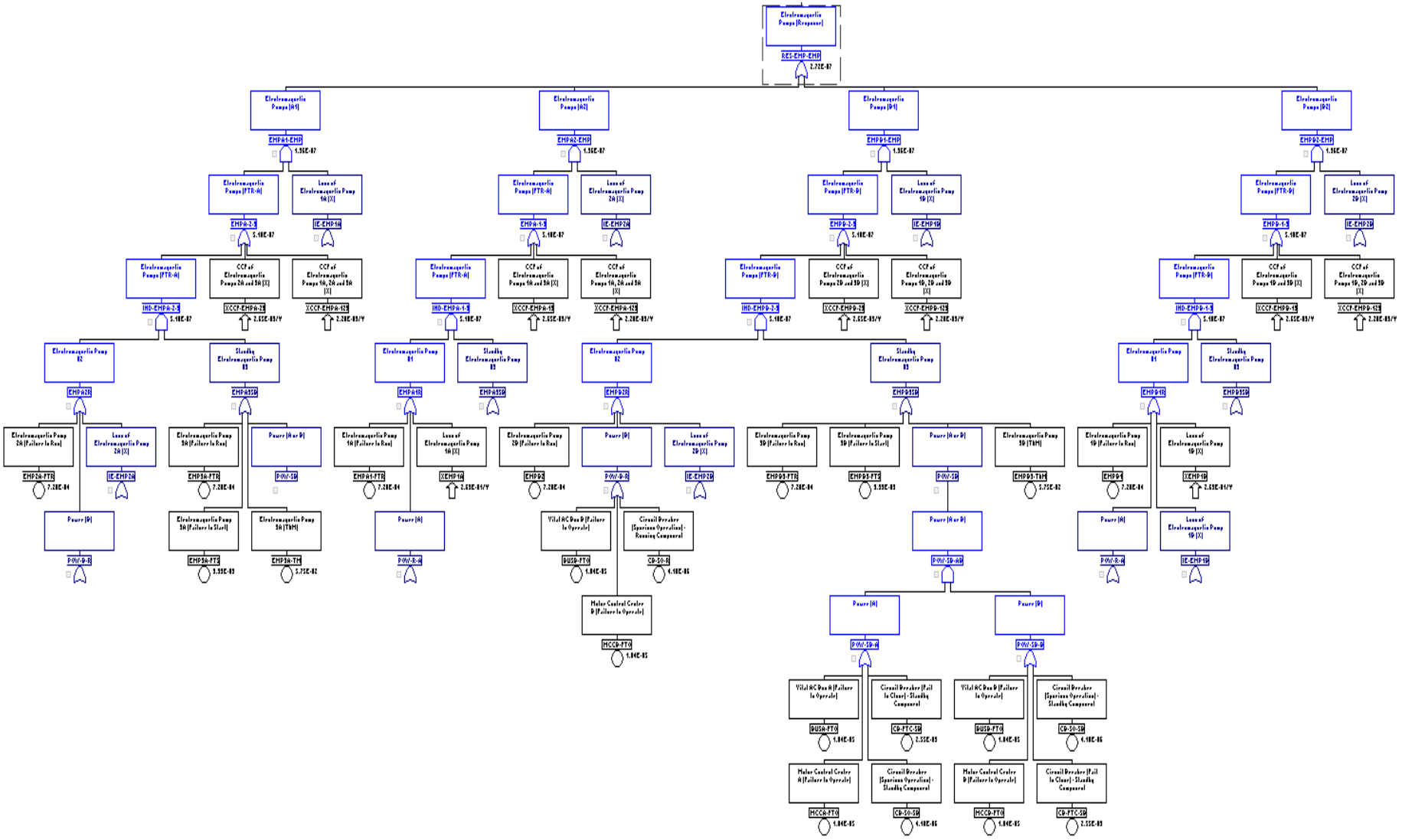

Figure A.6. System Response Model for Electromagnetic Pumps

Table A.3. Initiating Event Frequencies and Component/System Failure Rates used by the Model

Component and Failure Mode	Failure Rate	Initiator or System Failure	Assumption/Comments
Electromagnetic Pump (Failure to Run)	3.00E-05/hr	Both	Assumed unproven for NPP use. Failure rate somewhat higher than average.
Electromagnetic Pump (Failure to Start)	3.34E-03/dmd	System Failure	Assumed unproven for NPP use. Failure rate somewhat higher than average.
RVACS (Failure to Operate)	5.00E-07/hr	Both	Recovery of RVACS given it plugs was assumed to be 1E-1.
Intermediate Heat Exchanger (Tube Rupture)	8.70E-03/yr	Initiator	Assumed unproven for NPP use. Failure rate much higher than average.
Intermediate Loop Isolation Valve (Failure to Close)	7.00E-03/dmd	System Failure	Assumed to somewhat higher than NPP average. Motive power undefined.
Intermediate Loop Pump (Failure To Run)	2.00E-05/hr	Both	Failure rate assumed to be near NPP average for motor driven pumps.
Steam Generator (Tube Rupture)	8.76E-04/yr	Initiator	Assumed to be proven for NPP use. Failure rate lower than average.
SWR Pressure Relief System (Failure to Operate)	2.00E-04/dmd	System Failure	Failure rate assumed to be near NPP average for pressure relief systems.
Steam Drum	-	-	Failure of this passive component not modeled. Assumed to be small contributor to risk.
Feedwater Pump (Failure To Run)	1.00E-05/hr	Both	Failure rate assumed to be near NPP average for motor-driven pumps.
Steam Generator Louver (Failure To Open)	5.00E-02/hr	System Failure	Bounded by operator failure to open steam generator air flow louvers.
Turbine Generator	-	-	Assumed to be encompassed by reactor transient trip events.
Turbine Bypass Valve (Failure To Open)	1.00E-03/hr	System Failure	Failure rate assumed to be near NPP average.
Turbine Flow Control Valve	-	-	Assumed to be encompassed by reactor transient trip events.
Main Feedwater Pump (Failure To Run)	1.00E-05/hr	Both	Failure rate assumed to be near NPP average for motor-driven pumps.
Main Feedwater Heater	-	-	Assumed to be encompassed by reactor transient trip events.
Main Condensate Pump (Failure To Run)	1.00E-05/hr	Both	Failure rate assumed to be near NPP average for motor-driven pumps.
Emergency Diesel Generator (Failure To Start)	4.53E-03/ dmd	System Failure	Failure rate assumed to be near NPP average for emergency diesel generators.
Control Rod Drive Mechanism (Independent Failure)	5.78E-06/ dmd	System Failure	Failure rate assumed to be near NPP average for control rod drive mechanisms.
Trip Sensor (Independent Failure)	2.00E-15/ dmd	System Failure	Failure rate assumed to be near NPP average for trip sensors.
Trip Circuit Breaker (Independent Failure)	2.00E-16/ dmd	System Failure	Failure rate assumed to be near NPP average for trip circuit breakers.
Trip Setpoint (Independent Failure)	3.00E-15/ dmd	System Failure	Failure rate assumed to be near NPP average for trip setpoints.
Emergency Diesel Generator (Failure To Run During First Hour)	2.90E-03/ dmd	System Failure	Failure rate assumed to be near NPP average for emergency diesel generators.
Emergency Diesel Generator (Failure To Run)	8.48E-04/ dmd	System Failure	Failure rate assumed to be near NPP average for emergency diesel generators.

Component and Failure Mode	Failure Rate	Initiator or System Failure	Assumption/Comments
Motor Control Center (Failure to Operate)	4.34E-07/hr	System Failure	Failure rate assumed to be near NPP average for motor control centers.
Electrical Bus (Failure to Operate)	4.34E-07/hr	System Failure	Failure rate assumed to be near NPP average for electrical busses.
Circuit Breaker (Failure to Open/Close)	2.55E-03/hr	System Failure	Failure rate assumed to be near NPP average for circuit breakers.
Circuit Breaker (Spurious Operation)	1.71E-07/hr	System Failure	Failure rate assumed to be near NPP average for circuit breakers.
Motor-Operated Valve (Spurious Operation)	4.45E-08/hr	System Failure	Failure rate assumed to be near NPP average for motor-operated valves.
Reactor Transient (Trip)	2.50E-01/yr	Initiator	Failure rate assumed to be below average for NPP trips.

Note: Adapted from NUREG/CR-6928, Industry-Average Performance for Components and Initiating Events at U.S. Commercial Nuclear Power Plants (Eide et al. 2007).

A.3.5 Common Cause Failure Analysis

Common Cause Failures (CCF) occur when multiple (usually identical) components fail due to shared causes. A CCF event consists of component failures that meet four criteria:

- Two or more individual components fail or are degraded, including failures during demand, in-service testing or deficiencies that would have resulted in a failure if a demand signal had been received;
- Components fail within a selected period of time such that success of the PRA mission would be uncertain;
- Component failures result from a single shared cause and coupling mechanism; and
- A component failure occurs within the established component boundary.

The coupling mechanism classification generally consists of three major classes

- Hardware based
- Operation based
- Environment based.

In the PRA model developed for the simplified-model AdvSMR design, a parametric model known as the Alpha Factor model was used to model most CCF events. This model is a multi-parameter model that can handle any redundancy level and is based on ratios of failure rates, which make the assessment of its parameters easier when no statistical data are available. Alpha factors used by the PRA model are presented by component type and failure model in Table A.4.

Point value estimates representing the totality of common cause failure modes for trip circuit breakers, control rod drive mechanisms, trip setpoints, and trip sensors were used in modeling the reactor shutdown or protection system.

Table A.4. Common Cause Parameters used by the Model

Component and Failure Mode	CCCG	Alpha Factors
Electromagnetic Pump (Failure to Run)	3	α_1=9.72E-01 α_2=1.96E-02 α_3=8.44E-03
Intermediate Loop Isolation Valve (Failure to Close)	2	α_1=8.61E-01 α_2=1.39E-01
Feedwater Pump (Failure To Run)	2	α_1=8.80E-01 α_2=1.20E-01
Main Condensate Pump (Failure To Run)	2	α_1=8.80E-01 α_2=1.20E-01
Intermediate Loop Pump (Failure To Run)	2	α_1=9.90E-01 α_2=1.00E-02
Emergency Diesel Generator (Failure To Run)	2	α_1=9.60E-01 α_2=4.01E-02
Emergency Diesel Generator (Failure To Run During First Hour)	2	α_1=9.60E-01 α_2=4.01E-02
Emergency Diesel Generator (Failure To Start)	2	α_1=9.69E-01 α_2=3.12E-02

Note: Adapted from NUREG/CR-5497, Common-Cause Failure Parameter Estimations (Marshall et al. 2007).

A.3.6 Human Reliability Analysis

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. Types of human errors considered in a PRA include:

- Type A errors are made before the occurrence of the initiating event and have the potential to lead to the failure or unavailability of safety related equipment or systems.
- Type B errors that could lead to an initiating event.
- Type C errors are made during the performance of the critical actions that need to be carried out by plant operators after the occurrence of an initiating event.

For the PRA model developed for the simplified-model AdvSMR design, all safety and support systems are assumed to actuate and disengage automatically and as needed through use of a highly reliable supervisory control system. As a result, a detailed HRA was not performed; however, given a failure of RVACS caused by external events such as high winds, the opportunity for recovery (e.g., unplug radiating fins) by plant operators was assumed to be possible and modeled using a conservative screening human error probability.

A.3.7 Quantification

The resulting PRA model, which consists of a single fault tree logic model that characterizes all relevant accident sequences identified in Section A.3.2, was quantified using a fault tree software package (EPRI 2013) used extensively within the U.S. nuclear power industry. The Boolean expressions represented by the fault tree are reduced to arrive at the smallest combination of basic failure events (i.e.,

minimal cutsets) that result in a core damage event. The overall CDF for the simplified-model AdvSMR design was determined to be approximately 4.18E-07/yr based on 1358 cutsets for the power block, which consists of two modules, or 2.09E-07/yr based on 679 cutsets for an individual model. The top 100 cutsets, ranked according to CDF, are presented in Table A.5 for the power block and account for approximately 97% of the total CDF. The descriptions of all basic events that are modeled in the PRA and thus form the cutsets shown in Table A.5 are provided in Table A.6. The overall contribution to the overall CDF from each initiator identified in Table A.1 is shown in Figure A.7. Note, however, that some initiating events contribute negligibly to overall CDF and are therefore not presented in this figure.

In addition, an analysis was performed to determine the relative importance of each initiating or basic event to the overall CDF. This importance analysis considered the following four importance measures:

- RAW, which represents the relative risk increase assuming failure;
- RRW, which represents the relative risk reduction assuming perfect performance;
- F-V, which represents the fractional reduction in risk assuming perfect performance; and
- Birnbaum, which represents the difference in risk between perfect performance and assumed failure.

As discussed in Section A.1, importance measures are valuable in sorting out the most important component failure modes and initiating events. The results of this analysis are presented in Table A.6.

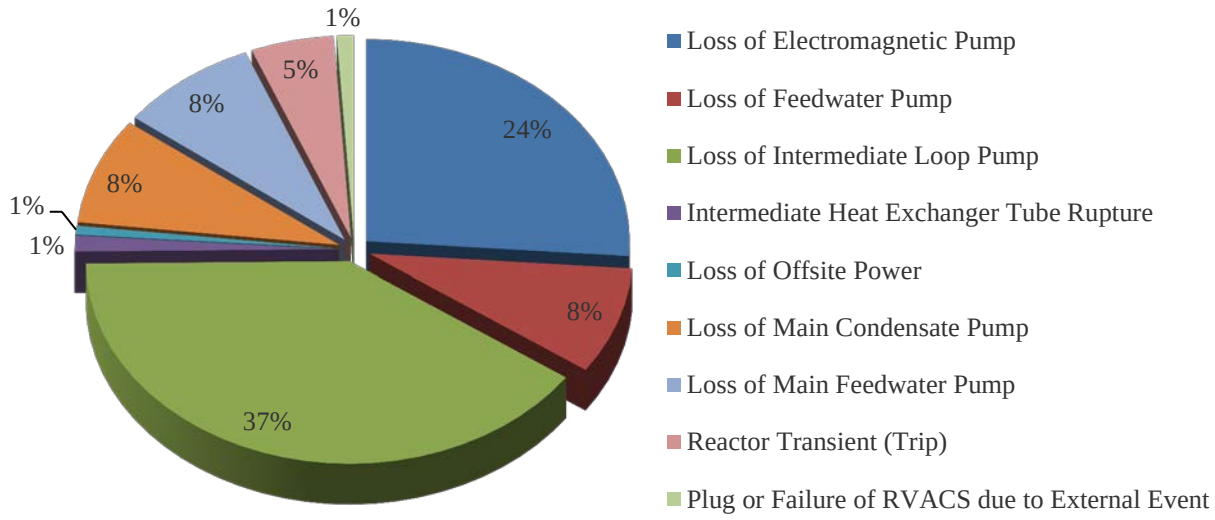

Figure A.7. Contribution of Each Initiating Event to Overall CDF

Table A.5. Dominant Cutsets for Simplified-Model AdvSMR PRA Model (Modules A and B)

CDF	Initiating Event	Subsequent Component/System Failures	
2.74E-08	%CCF-EMPA-123	RVACSA	
2.74E-08	%CCF-EMPB-123	RVACSB	
2.12E-08	%CCF-IMHPA-12	RVACSA	
2.12E-08	%CCF-IMHPB-12	RVACSB	
2.02E-08	%IMHP1A	IMHP2A-TM	RVACSA
2.02E-08	%IMHP1B	IMHP2B-TM	RVACSB
2.02E-08	%IMHP2A	IMHP1A-TM	RVACSA
2.02E-08	%IMHP2B	IMHP1B-TM	RVACSB
1.05E-08	%SGA	RVACSA	
1.05E-08	%SGB	RVACSB	
9.12E-09	%EMP1A	CCF-CDRM-RSS	
9.12E-09	%EMP1B	CCF-CDRM-RSS	
9.12E-09	%EMP2A	CCF-CDRM-RSS	
9.12E-09	%EMP2B	CCF-CDRM-RSS	
8.68E-09	%RTTA	CCF-CDRM-RSS	
8.68E-09	%RTTB	CCF-CDRM-RSS	
7.17E-09	%CCF-FWPA-12	RVACSA	SGLVA
7.17E-09	%CCF-FWPB-12	RVACSB	SGLVB
7.17E-09	%CCF-MCPA-12	RVACSA	SGLVA
7.17E-09	%CCF-MCPB-12	RVACSB	SGLVB
7.17E-09	%CCF-MFWPA-12	RVACSA	SGLVA
7.17E-09	%CCF-MFWPB-12	RVACSB	SGLVB
6.08E-09	%IMHP1A	CCF-CDRM-RSS	
6.08E-09	%IMHP1B	CCF-CDRM-RSS	
6.08E-09	%IMHP2A	CCF-CDRM-RSS	
6.08E-09	%IMHP2B	CCF-CDRM-RSS	
3.04E-09	%FWP1A	CCF-CDRM-RSS	
3.04E-09	%FWP1B	CCF-CDRM-RSS	
3.04E-09	%FWP2A	CCF-CDRM-RSS	
3.04E-09	%FWP2B	CCF-CDRM-RSS	
3.04E-09	%MCP1A	CCF-CDRM-RSS	
3.04E-09	%MCP1B	CCF-CDRM-RSS	
3.04E-09	%MCP2A	CCF-CDRM-RSS	
3.04E-09	%MCP2B	CCF-CDRM-RSS	
3.04E-09	%MFWP1A	CCF-CDRM-RSS	
3.04E-09	%MFWP1B	CCF-CDRM-RSS	
3.04E-09	%MFWP2A	CCF-CDRM-RSS	
3.04E-09	%MFWP2B	CCF-CDRM-RSS	
2.00E-09	%RVACSEE	HR-RVACSA	SGLVA
2.00E-09	%RVACSEE	HR-RVACSB	SGLVB
1.83E-09	%CCF-EMPA-12	EMP3A-TM	RVACSA
1.83E-09	%CCF-EMPB-12	EMPB3-T&M	RVACSB
1.25E-09	%LOP	CCF-CDRM-RSS	
1.22E-09	%SGA	IHIVA1	SWRPPSA1
1.22E-09	%SGA	IHIVA1	SWRPPSA2
1.22E-09	%SGA	IHIVA2	SWRPPSA1
1.22E-09	%SGA	IHIVA2	SWRPPSA2
1.22E-09	%SGB	IHIVB1	SWRPPSB1
1.22E-09	%SGB	IHIVB1	SWRPPSB2
1.22E-09	%SGB	IHIVB2	SWRPPSB1
1.22E-09	%SGB	IHIVB2	SWRPPSB2
1.01E-09	%IMHXA	IMHP1A-TM	RVACSA

CDF	Initiating Event	Subsequent Component/System Failures		
1.01E-09	%IMHXA	IMHP2A-TM	RVACSA	
1.01E-09	%IMHXB	IMHP1B-TM	RVACSB	
1.01E-09	%IMHXB	IMHP2B-TM	RVACSB	
1.01E-09	%FWP1A	FWP2A-TM	RVACSA	SGLVA
1.01E-09	%FWP1B	FWP2B-TM	RVACSB	SGLVB
1.01E-09	%FWP2A	FWP1A-TM	RVACSA	SGLVA
1.01E-09	%FWP2B	FWP1B-TM	RVACSB	SGLVB
1.01E-09	%MCP1A	MCP2A-TM	RVACSA	SGLVA
1.01E-09	%MCP1B	MCP2B-TM	RVACSB	SGLVB
1.01E-09	%MCP2A	MCP1A-TM	RVACSA	SGLVA
1.01E-09	%MCP2B	MCP1B-TM	RVACSB	SGLVB
1.01E-09	%MFWP1A	MFWP2A-TM	RVACSA	SGLVA
1.01E-09	%MFWP1B	MFWP2B-TM	RVACSB	SGLVB
1.01E-09	%MFWP2A	MFWP1A-TM	RVACSA	SGLVA
1.01E-09	%MFWP2B	MFWP1B-TM	RVACSB	SGLVB
1.01E-09	%IMHP1A	IMHP2A	RVACSA	
1.01E-09	%IMHP1B	IMHP2B	RVACSB	
1.01E-09	%IMHP2A	IMHP1A	RVACSA	
1.01E-09	%IMHP2B	IMHP1B	RVACSB	
6.04E-10	%EMP1A	DEP-TSP-RPS		
6.04E-10	%EMP1B	DEP-TSP-RPS		
6.04E-10	%EMP2A	DEP-TSP-RPS		
6.04E-10	%EMP2B	DEP-TSP-RPS		
5.75E-10	%RTTA	DEP-TSP-RPS		
5.75E-10	%RTTB	DEP-TSP-RPS		
4.14E-10	%CCF-FWPA-12	CCF-CDRM-RSS		
4.14E-10	%CCF-FWPB-12	CCF-CDRM-RSS		
4.14E-10	%CCF-MCPA-12	CCF-CDRM-RSS		
4.14E-10	%CCF-MCPB-12	CCF-CDRM-RSS		
4.14E-10	%CCF-MFWPA-12	CCF-CDRM-RSS		
4.14E-10	%CCF-MFWPB-12	CCF-CDRM-RSS		
4.03E-10	%IMHP1A	DEP-TSP-RPS		
4.03E-10	%IMHP1B	DEP-TSP-RPS		
4.03E-10	%IMHP2A	DEP-TSP-RPS		
4.03E-10	%IMHP2B	DEP-TSP-RPS		
3.04E-10	%IMHXA	CCF-CDRM-RSS		
3.04E-10	%IMHXB	CCF-CDRM-RSS		
2.68E-10	%LOP	CCF-EDG-FTR	RVACSA	
2.68E-10	%LOP	CCF-EDG-FTR	RVACSB	
2.63E-10	%EMP1A	CCF-TSENS-RPS		
2.63E-10	%EMP1B	CCF-TSENS-RPS		
2.63E-10	%EMP2A	CCF-TSENS-RPS		
2.63E-10	%EMP2B	CCF-TSENS-RPS		
2.50E-10	%RTTA	CCF-TSENS-RPS		
2.50E-10	%RTTB	CCF-TSENS-RPS		
2.01E-10	%FWP1A	DEP-TSP-RPS		
2.01E-10	%FWP1B	DEP-TSP-RPS		
2.01E-10	%FWP2A	DEP-TSP-RPS		
4.06E-07[(a)]				

(a) Total CDF of the top 100 cutsets.

Table A.6. Basic Events Descriptions and Importance Analysis Results

Basic Event Name	Probability	F-V	Birnbaum	RRW	RAW	Basic Event Description
%CCF-EMPA-12	2.65E-03	5.13E-03	8.08E-07	1.01E+00	2.93E+00	CCF of Electromagnetic Pumps 1A and 2A (Initiating Event)
%CCF-EMPA-123	2.28E-03	6.58E-02	1.20E-05	1.07E+00	2.98E+01	CCF of Electromagnetic Pumps 1A, 2A and 3A (Initiating Event)
%CCF-EMPA-13	2.65E-03	2.50E-04	3.93E-08	1.00E+00	1.09E+00	CCF of Electromagnetic Pumps 1A and 3A (Initiating Event)
%CCF-EMPA-23	2.65E-03	2.50E-04	3.93E-08	1.00E+00	1.09E+00	CCF of Electromagnetic Pumps 2A and 3A (Initiating Event)
%CCF-EMPB-12	2.65E-03	5.13E-03	8.08E-07	1.01E+00	2.93E+00	CCF of Electromagnetic Pumps 1B and 2B (Initiating Event)
%CCF-EMPB-123	2.28E-03	6.58E-02	1.20E-05	1.07E+00	2.98E+01	CCF of Electromagnetic Pumps 1B, 2B and 3B (Initiating Event)
%CCF-EMPB-13	2.65E-03	2.50E-04	3.93E-08	1.00E+00	1.09E+00	CCF of Electromagnetic Pumps 1B and 3B (Initiating Event)
%CCF-EMPB-23	2.65E-03	2.50E-04	3.93E-08	1.00E+00	1.09E+00	CCF of Electromagnetic Pumps 2B and 3B (Initiating Event)
%CCF-FWPA-12	1.19E-02	1.83E-02	6.39E-07	1.02E+00	2.51E+00	CCF Involving Loss of Feedwater Pumps 1A and 2A (Initiating Event)
%CCF-FWPB-12	1.19E-02	1.83E-02	6.39E-07	1.02E+00	2.51E+00	CCF Involving Loss of Feedwater Pumps 1A and 2A (Initiating Event)
%CCF-IMHPA-12	1.77E-03	5.10E-02	1.20E-05	1.05E+00	2.98E+01	CCF Involving Loss of Intermediate Loop Pump 1A and 2A (Initiating Event)
%CCF-IMHPB-12	1.77E-03	5.10E-02	1.20E-05	1.05E+00	2.98E+01	CCF Involving Loss of Intermediate Loop Pump 1B and 2B (Initiating Event)
%CCF-MCPA-12	1.19E-02	1.83E-02	6.39E-07	1.02E+00	2.51E+00	CCF Involving Loss of Main Condensate Pumps 1A and 2A (Initiating Event)
%CCF-MCPB-12	1.19E-02	1.83E-02	6.39E-07	1.02E+00	2.51E+00	CCF Involving Loss of Main Condensate Pumps 1B and 2B (Initiating Event)
%CCF-MFWPA-12	1.19E-02	1.83E-02	6.39E-07	1.02E+00	2.51E+00	CCF Involving Loss of Main Feedwater Pumps 1A and 2A (Initiating Event)
%CCF-MFWPB-12	1.19E-02	1.83E-02	6.39E-07	1.02E+00	2.51E+00	CCF Involving Loss of Main Feedwater Pumps 1B and 2B (Initiating Event)
%EMP1A	2.63E-01	2.47E-02	3.93E-08	1.03E+00	1.07E+00	Loss of Electromagnetic Pump 1A (Initiating Event)
%EMP1B	2.63E-01	2.47E-02	3.93E-08	1.03E+00	1.07E+00	Loss of Electromagnetic Pump 1B (Initiating Event)
%EMP2A	2.63E-01	2.47E-02	3.93E-08	1.03E+00	1.07E+00	Loss of Electromagnetic Pump 2A (Initiating Event)
%EMP2B	2.63E-01	2.47E-02	3.93E-08	1.03E+00	1.07E+00	Loss of Electromagnetic Pump 2B (Initiating Event)
%FWP1A	8.76E-02	1.06E-02	5.04E-08	1.01E+00	1.11E+00	Loss of Feedwater Pump 1A (Initiating Event)

Basic Event Name	Probability	F-V	Birnbaum	RRW	RAW	Basic Event Description
%FWP1B	8.76E-02	1.06E-02	5.04E-08	1.01E+00	1.11E+00	Loss of Feedwater Pump 1B (Initiating Event)
%FWP2A	8.76E-02	1.06E-02	5.04E-08	1.01E+00	1.11E+00	Loss of Feedwater Pump 2A (Initiating Event)
%FWP2B	8.76E-02	1.06E-02	5.04E-08	1.01E+00	1.11E+00	Loss of Feedwater Pump 2B (Initiating Event)
%IMHP1A	1.75E-01	6.72E-02	1.60E-07	1.07E+00	1.32E+00	Loss of Intermediate Loop Pump 1A (Initiating Event)
%IMHP1B	1.75E-01	6.72E-02	1.60E-07	1.07E+00	1.32E+00	Loss of Intermediate Loop Pump 1B (Initiating Event)
%IMHP2A	1.75E-01	6.72E-02	1.60E-07	1.07E+00	1.32E+00	Loss of Intermediate Loop Pump 2A (Initiating Event)
%IMHP2B	1.75E-01	6.72E-02	1.60E-07	1.07E+00	1.32E+00	Loss of Intermediate Loop Pump 2B (Initiating Event)
%IMHXA	8.76E-03	5.91E-03	2.82E-07	1.01E+00	1.67E+00	Intermediate Heat Exchanger Tube Rupture on Module A (Initiating Event)
%IMHXB	8.76E-03	5.91E-03	2.82E-07	1.01E+00	1.67E+00	Intermediate Heat Exchanger Tube Rupture on Module B (Initiating Event)
%LOP	3.59E-02	6.58E-03	7.65E-08	1.01E+00	1.18E+00	Loss of Offsite Power (Initiating Event)
%MCP1A	8.76E-02	1.06E-02	5.04E-08	1.01E+00	1.11E+00	Loss of Main Condensate Pump 1A (Initiating Event)
%MCP1B	8.76E-02	1.06E-02	5.04E-08	1.01E+00	1.11E+00	Loss of Main Condensate Pump 1B (Initiating Event)
%MCP2A	8.76E-02	1.06E-02	5.04E-08	1.01E+00	1.11E+00	Loss of Main Condensate Pump 2A (Initiating Event)
%MCP2B	8.76E-02	1.06E-02	5.04E-08	1.01E+00	1.11E+00	Loss of Main Condensate Pump 2B (Initiating Event)
%MFWP1A	8.76E-02	1.06E-02	5.04E-08	1.01E+00	1.11E+00	Loss of Main Feedwater Pump 1A (Initiating Event)
%MFWP1B	8.76E-02	1.06E-02	5.04E-08	1.01E+00	1.11E+00	Loss of Main Feedwater Pump 1B (Initiating Event)
%MFWP2A	8.76E-02	1.06E-02	5.04E-08	1.01E+00	1.11E+00	Loss of Main Feedwater Pump 2A (Initiating Event)
%MFWP2B	8.76E-02	1.06E-02	5.04E-08	1.01E+00	1.11E+00	Loss of Main Feedwater Pump 2B (Initiating Event)
%RTTA	2.50E-01	2.35E-02	3.93E-08	1.02E+00	1.07E+00	Reactor Transient Trip on Module A (Initiating Event)
%RTTB	2.50E-01	2.35E-02	3.93E-08	1.02E+00	1.07E+00	Reactor Transient Trip on Module B (Initiating Event)
%RVACSEE	4.00E-07	9.56E-03	9.98E-03	1.01E+00	2.39E+04	Plug or Failure of RVACS on Modules A and B due to External Event (Initiating Event)
%SGA	8.76E-04	3.80E-02	1.81E-05	1.04E+00	4.43E+01	Steam Generator Tube Rupture on Module A (Initiating Event)
%SGB	8.76E-04	3.80E-02	1.81E-05	1.04E+00	4.43E+01	Steam Generator Tube Rupture on Module B (Initiating Event)
BUSA-FTO	1.04E-05	1.50E-04	5.84E-06	1.00E+00	1.50E+01	Vital AC Bus A (Failure to Operate)
BUSB-FTO	1.04E-05	1.50E-04	5.84E-06	1.00E+00	1.50E+01	Vital AC Bus B (Failure to Operate)

Basic Event Name	Probability	F-V	Birnbaum	RRW	RAW	Basic Event Description
CB-FTC-SB	2.55E-03	4.50E-04	7.31E-08	1.00E+00	1.18E+00	Circuit Breaker (Fail to Close) - Standby Component
CB-SO-R	4.10E-06	1.10E-04	1.08E-05	1.00E+00	2.68E+01	Circuit Breaker (Spurious Operation) - Running Component
CB-SO-SB	4.10E-06	0.00E+00	7.31E-08	1.00E+00	1.18E+00	Circuit Breaker (Spurious Operation) - Standby Component
CCF-CDRM-RSS	3.47E-08	2.87E-01	3.45E+00	1.40E+00	8.27E+06	Control Rod Drive Mechanisms (Common Cause Failure)
CCF-EDG-FTR	6.22E-04	1.28E-03	8.62E-07	1.00E+00	3.06E+00	CCF Involving EDGs (Failure to Run)
CCF-EDG-FTR-1HR	9.33E-05	1.90E-04	8.62E-07	1.00E+00	3.06E+00	CCF Involving EDGs (Failure to Run during First Hour)
CCF-EDG-FTS	1.46E-04	3.00E-04	8.62E-07	1.00E+00	3.06E+00	CCF Involving EDGs (Failure to Start)
CCF-IHIVA	1.13E-03	9.50E-04	3.50E-07	1.00E+00	1.84E+00	Intermediate Isolation Valves 1A and 2A (Failure to Close)
CCF-IHIVB	1.13E-03	9.50E-04	3.50E-07	1.00E+00	1.84E+00	Intermediate Isolation Valves 1B and 2B (Failure to Close)
CCF-TSENS-RPS	1.00E-09	8.27E-03	3.45E+00	1.01E+00	8.27E+06	Trip Sensors (Common Cause Failure)
CDRM1-RSS	5.78E-06	1.38E-03	9.98E-05	1.00E+00	2.40E+02	Control Rod Drive Mechanism 1 (Failure to Insert)
CDRM2-RSS	5.78E-06	1.38E-03	9.98E-05	1.00E+00	2.40E+02	Control Rod Drive Mechanism 2 (Failure to Insert)
CDRM3-RSS	5.78E-06	1.38E-03	9.98E-05	1.00E+00	2.40E+02	Control Rod Drive Mechanism 3 (Failure to Insert)
CDRM4-RSS	5.78E-06	1.38E-03	9.98E-05	1.00E+00	2.40E+02	Control Rod Drive Mechanism 4 (Failure to Insert)
CDRM5-RSS	5.78E-06	1.38E-03	9.98E-05	1.00E+00	2.40E+02	Control Rod Drive Mechanism 5 (Failure to Insert)
CDRM6-RSS	5.78E-06	1.38E-03	9.98E-05	1.00E+00	2.40E+02	Control Rod Drive Mechanism 6 (Failure to Insert)
DEP-TCB-RPS	2.00E-10	1.65E-03	3.45E+00	1.00E+00	8.27E+06	Trip Circuit Breakers (Common Cause Failure)
DEP-TSP-RPS	2.30E-09	1.90E-02	3.45E+00	1.02E+00	8.27E+06	Trip Setpoints (Common Cause Failure)
EDGA-FTR	1.93E-02	1.07E-03	2.30E-08	1.00E+00	1.05E+00	Emergency Diesel A (Fails to Run after First Hour)
EDGA-FTR-1HR	2.90E-03	1.60E-04	2.30E-08	1.00E+00	1.06E+00	Emergency Diesel A (Failure to Load and Run during First Hour)
EDGA-FTS	4.52E-03	2.50E-04	2.30E-08	1.00E+00	1.06E+00	Emergency Diesel A (Failure to Start)
EDGB-FTR	1.93E-02	1.07E-03	2.30E-08	1.00E+00	1.05E+00	Emergency Diesel B (Fails to Run after First Hour)
EDGB-FTR-1HR	2.90E-03	1.60E-04	2.30E-08	1.00E+00	1.06E+00	Emergency Diesel B (Failure to Load and Run during First Hour)
EDGB-FTS	4.52E-03	2.50E-04	2.30E-08	1.00E+00	1.06E+00	Emergency Diesel B (Failure to Start)
EMP2A-FTR	7.20E-04	3.50E-04	2.04E-07	1.00E+00	1.49E+00	Electromagnetic Pump 2A (Failure to Run)

Basic Event Name	Probability	F-V	Birnbaum	RRW	RAW	Basic Event Description
EMP3A-FTR	7.20E-04	6.00E-05	3.65E-08	1.00E+00	1.09E+00	Electromagnetic Pump 3A (Failure to Run)
EMP3A-FTS	3.33E-03	2.90E-04	3.65E-08	1.00E+00	1.09E+00	Electromagnetic Pump 3A (Failure to Start)
EMP3A-TM	5.75E-02	5.03E-03	3.65E-08	1.01E+00	1.08E+00	Electromagnetic Pump 3A (T&M)
EMPA1-FTR	7.20E-04	3.50E-04	2.04E-07	1.00E+00	1.49E+00	Electromagnetic Pump 1A (Failure to Run)
EMPB1	7.20E-04	3.50E-04	2.04E-07	1.00E+00	1.49E+00	Electromagnetic Pump 1B (Failure to Run)
EMPB2	7.20E-04	3.50E-04	2.04E-07	1.00E+00	1.49E+00	Electromagnetic Pump 2B (Failure to Run)
EMPB3-FTR	7.20E-04	6.00E-05	3.65E-08	1.00E+00	1.09E+00	Electromagnetic Pump 3B (Failure to Run)
EMPB3-FTS	3.33E-03	2.90E-04	3.65E-08	1.00E+00	1.09E+00	Electromagnetic Pump 3B (Failure to Start)
EMPB3-T&M	5.75E-02	5.03E-03	3.65E-08	1.01E+00	1.08E+00	Electromagnetic Pump 3B (T&M)
FWP1A	2.40E-04	3.00E-05	5.26E-08	1.00E+00	1.13E+00	Feedwater Pump 1A (Failure to Run)
FWP1A-TM	1.92E-02	2.42E-03	5.26E-08	1.00E+00	1.12E+00	Feedwater Pump 1A (T&M)
FWP1B	2.40E-04	3.00E-05	5.26E-08	1.00E+00	1.13E+00	Feedwater Pump 1B (Failure to Run)
FWP1B-TM	1.92E-02	2.42E-03	5.26E-08	1.00E+00	1.12E+00	Feedwater Pump 1B (T&M)
FWP2A	2.40E-04	3.00E-05	5.26E-08	1.00E+00	1.13E+00	Feedwater Pump 2A (Failure to Run)
FWP2A-TM	1.92E-02	2.42E-03	5.26E-08	1.00E+00	1.12E+00	Feedwater Pump 2A (T&M)
FWP2B	2.40E-04	3.00E-05	5.26E-08	1.00E+00	1.13E+00	Feedwater Pump 2B (Failure to Run)
FWP2B-TM	1.92E-02	2.42E-03	5.26E-08	1.00E+00	1.12E+00	Feedwater Pump 2B (T&M)
HR-RVACSA	1.00E-01	4.79E-03	1.99E-08	1.00E+00	1.04E+00	Op Action - Failure to Recover RVACS
HR-RVACSB	1.00E-01	4.79E-03	1.99E-08	1.00E+00	1.04E+00	Op Action - Failure to Recover RVACS
IHIVA-SO1	1.07E-06	0.00E+00	3.50E-07	1.00E+00	1.84E+00	Intermediate Isolation Valve 1A (Sprious Operation)
IHIVA-SO2	1.07E-06	0.00E+00	3.50E-07	1.00E+00	1.84E+00	Intermediate Isolation Valve 2A (Sprious Operation)
IHIVA1	6.98E-03	5.85E-03	3.50E-07	1.01E+00	1.83E+00	Intermediate Isolation Valve 1A (Failure to Close)
IHIVA2	6.98E-03	5.85E-03	3.50E-07	1.01E+00	1.83E+00	Intermediate Isolation Valve 2A (Failure to Close)
IHIVB-SO1	1.07E-06	0.00E+00	3.50E-07	1.00E+00	1.84E+00	Intermediate Isolation Valve 1B (Sprious Operation)
IHIVB-SO2	1.07E-06	0.00E+00	3.50E-07	1.00E+00	1.84E+00	Intermediate Isolation Valve 2B (Sprious Operation)
IHIVB1	6.98E-03	5.85E-03	3.50E-07	1.01E+00	1.83E+00	Intermediate Isolation Valve 1B (Failure to Close)
IHIVB2	6.98E-03	5.85E-03	3.50E-07	1.01E+00	1.83E+00	Intermediate Isolation Valve 2B (Failure to Close)
IMHP1A	4.80E-04	2.54E-03	2.21E-06	1.00E+00	6.29E+00	Intermediate Loop Pump 1A (Failure to Run)
IMHP1A-TM	9.62E-03	5.08E-02	2.21E-06	1.05E+00	6.24E+00	Intermediate Loop Pump 1A (T&M)

Basic Event Name	Probability	F-V	Birnbaum	RRW	RAW	Basic Event Description
IMHP1B	4.80E-04	2.54E-03	2.21E-06	1.00E+00	6.29E+00	Intermediate Loop Pump 1B (Failure to Run)
IMHP1B-TM	9.62E-03	5.08E-02	2.21E-06	1.05E+00	6.24E+00	Intermediate Loop Pump 1B (T&M)
IMHP2A	4.80E-04	2.54E-03	2.21E-06	1.00E+00	6.29E+00	Intermediate Loop Pump 2A (Failure to Run)
IMHP2A-TM	9.62E-03	5.08E-02	2.21E-06	1.05E+00	6.24E+00	Intermediate Loop Pump 2A (T&M)
IMHP2B	4.80E-04	2.54E-03	2.21E-06	1.00E+00	6.29E+00	Intermediate Loop Pump 2B (Failure to Run)
IMHP2B-TM	9.62E-03	5.08E-02	2.21E-06	1.05E+00	6.24E+00	Intermediate Loop Pump 2B (T&M)
IND-TCB-RPS	2.00E-16	0.00E+00	3.45E+00	1.00E+00	8.27E+06	Trip Circuit Breakers (Independent Failure)
IND-TSENS-RPS	2.00E-15	0.00E+00	3.45E+00	1.00E+00	8.27E+06	Trip Sensors (Independent Failure)
IND-TSPS-RPS	3.00E-15	0.00E+00	3.45E+00	1.00E+00	8.27E+06	Trip Setpoints (Independent Failure)
MCCA-FTO	1.04E-05	1.50E-04	5.84E-06	1.00E+00	1.50E+01	Motor Control Center A (Failure to Operate)
MCCB-FTO	1.04E-05	1.50E-04	5.84E-06	1.00E+00	1.50E+01	Motor Control Center B (Failure to Operate)
MCP1A	2.40E-04	3.00E-05	5.26E-08	1.00E+00	1.13E+00	Loss of Main Condensate Pump 1A (Failure to Run)
MCP1A-TM	1.92E-02	2.42E-03	5.26E-08	1.00E+00	1.12E+00	Loss of Main Condensate Pump 1A (T&M)
MCP1B	2.40E-04	3.00E-05	5.26E-08	1.00E+00	1.13E+00	Loss of Main Condensate Pump 1B (Failure to Run)
MCP1B-TM	1.92E-02	2.42E-03	5.26E-08	1.00E+00	1.12E+00	Loss of Main Condensate Pump 1B (T&M)
MCP2A	2.40E-04	3.00E-05	5.26E-08	1.00E+00	1.13E+00	Loss of Main Condensate Pump 2A (Failure to Run)
MCP2A-TM	1.92E-02	2.42E-03	5.26E-08	1.00E+00	1.12E+00	Loss of Main Condensate Pump 2A (T&M)
MCP2B	2.40E-04	3.00E-05	5.26E-08	1.00E+00	1.13E+00	Loss of Main Condensate Pump 2B (Failure to Run)
MCP2B-TM	1.92E-02	2.42E-03	5.26E-08	1.00E+00	1.12E+00	Loss of Main Condensate Pump 2B (T&M)
MFWP1A	2.40E-04	3.00E-05	5.26E-08	1.00E+00	1.13E+00	Main Feedwater Pump 1A (Failure to Run)
MFWP1A-TM	1.92E-02	2.42E-03	5.26E-08	1.00E+00	1.12E+00	Main Feedwater Pump 1A (T&M)
MFWP1B	2.40E-04	3.00E-05	5.26E-08	1.00E+00	1.13E+00	Main Feedwater Pump 1B (Failure to Run)
MFWP1B-TM	1.92E-02	2.42E-03	5.26E-08	1.00E+00	1.12E+00	Main Feedwater Pump 1B (T&M)
MFWP2A	2.40E-04	3.00E-05	5.26E-08	1.00E+00	1.13E+00	Main Feedwater Pump 2A (Failure to Run)
MFWP2A-TM	1.92E-02	2.42E-03	5.26E-08	1.00E+00	1.12E+00	Main Feedwater Pump 2A (T&M)
MFWP2B	2.40E-04	3.00E-05	5.26E-08	1.00E+00	1.13E+00	Main Feedwater Pump 2B (Failure to Run)
MFWP2B-TM	1.92E-02	2.42E-03	5.26E-08	1.00E+00	1.12E+00	Main Feedwater Pump 2B (T&M)

Basic Event Name	Probability	F-V	Birnbaum	RRW	RAW	Basic Event Description
RVACSA	1.20E-05	3.22E-01	1.12E-02	1.48E+00	2.69E+04	Reactor Vessel Auxiliary Cooling System A (Failure to Operate)
RVACSB	1.20E-05	3.22E-01	1.12E-02	1.48E+00	2.69E+04	Reactor Vessel Auxiliary Cooling System B (Failure to Operate)
SGLVA	5.00E-02	7.14E-02	5.96E-07	1.08E+00	2.36E+00	Steam Generator Louvers A (Failure to Open)
SGLVB	5.00E-02	7.14E-02	5.96E-07	1.08E+00	2.36E+00	Steam Generator Louvers B (Failure to Open)
SWRPPSA1	2.00E-04	6.35E-03	1.32E-05	1.01E+00	3.26E+01	Sodium-Water-Reaction Pressure Relief Valve 1A (Failure to Open)
SWRPPSA2	2.00E-04	6.35E-03	1.32E-05	1.01E+00	3.26E+01	Sodium-Water-Reaction Pressure Relief Valve 2A (Failure to Open)
SWRPPSB1	2.00E-04	6.35E-03	1.32E-05	1.01E+00	3.26E+01	Sodium-Water-Reaction Pressure Relief Valve 1B (Failure to Open)
SWRPPSB2	2.00E-04	6.35E-03	1.32E-05	1.01E+00	3.26E+01	Sodium-Water-Reaction Pressure Relief Valve 2B (Failure to Open)
TBVFTO	1.00E-03	7.20E-04	3.00E-07	1.00E+00	1.72E+00	Turbine Bypass Valve (Failure to Open)

Appendix B

FFTF Component Reliability Effort

Appendix B

FFTF Component Reliability Effort

An initial methodology for enhanced risk monitors (ERMs) is described in the main document that integrates real-time information about equipment condition and probability of failure into risk monitors to provide an assessment of dynamic risk as plant equipment ages. An important aspect of ERM is the inclusion of uncertainty within the ERM framework. Several sources of uncertainty exist when estimating the probability of failure, including uncertainty regarding the specific condition of the component, uncertainty in the probability of failure, and uncertainty in the time-to-failure. One way to address these sources of ERM uncertainty is through evaluation of real plant data.

The Fast Flux Test Facility (FFTF) was the most recent liquid metal reactor (LMR) to operate in the United States. The FFTF was located on the U.S. Government's Department of Energy (DOE) Hanford Site near Richland, Washington, and was operated successfully from 1982 to 1992. Safe, reliable, and economic operation of the FFTF was achieved through administrative controls, technical specifications, and operating procedures, even with a demanding test schedule as a liquid metal irradiation test reactor. The high level of operating efficiency of FFTF is a potential source of vital data on the performance of liquid sodium as a safe and efficient heat transport medium that confirms the reliability of many of its large-scale components. The ten years of successful operation of the FFTF provided a very useful framework that could potentially be used for determining the reliability of LMR technology components. A potential advantage of raw data sources like FFTF is the ability to track component reliability over time. FFTF sources of reliability data are being compiled and evaluated for applicability. Efforts to recover FFTF data useful for verifying ERM methodology have focused on locating the FFTF input to the Component Reliability Data Organization (CREDO) database records.

Processed CREDO component failure rate information has been identified as a source of information for developing the simplified ERM framework AdvSMR PRA model. A subset of several hundred significant events collected and categorized during a preliminary FFTF PRA effort has been recovered and is being evaluated for component reliability information. Such component reliability data is being evaluated as a way to validate the proposed methodology for ERM.

B.1 Background on FFTF

Conceptual design of the FFTF began in 1965, followed by a period of construction and acceptance testing that ended with first cycle operations in 1982. FFTF operations extended for a decade until it was shut down in 1992. FFTF was the most instrumented reactor in the world and had an excellent data monitoring and acquisition system. DOE investment in the design and operation of FFTF easily exceeds $10B.

The plan to build FFTF began to take shape in 1967 when the Hanford site at Richland, Washington, was chosen as the home of the first large-scale liquid metal test reactor. The plan was culminated on April 30, 1982, with dedication of the FFTF. In 1970, the DOE selected Westinghouse Hanford Company, a wholly owned subsidiary of the Westinghouse Electric Corporation, to manage the design, construction, and operation of the FFTF as part of the Hanford Engineering Development Laboratory.

The Advanced Reactors Division of the Westinghouse Electric Corporation, Pittsburgh, Pennsylvania, was the reactor designer; and Bechtel Power Corporation, San Francisco, California, was the architect engineer and construction manager. In addition, more than 300 companies across the nation provided components, materials, and fuel for the FFTF.

The primary mission of the FFTF was to test full-size nuclear fuels and components typical of those to be found in a commercial liquid metal reactor. To accomplish this mission, the DOE established two fundamental objectives. First, the reactor plant technology would support the liquid metal reactor industry by developing fuel assemblies, control rods, and other core components whose lifespans could be proven to be economical in commercial power-generating applications. Second, the reliability of the FFTF would be proven by matching or exceeding the operational performance of commercial light water plants. Safe, reliable, and economic operation of the FFTF was achieved through administrative controls, technical specifications, and operating procedures. The high level of operating efficiency of FFTF provided vital data on the performance of liquid sodium as a safe and efficient heat transport medium and confirmed the reliability of many of its large-scale components.

The FFTF plant was an 86,103 sq. ft. complex of buildings and equipment arranged around a reactor containment building. The reactor was located in a shielded cell in the center of the containment building. Heat was removed from the reactor by liquid sodium circulating under low pressure through three primary coolant loops. (This is in contrast to conventional reactor plants that use water circulated under high pressure.) An intermediate heat exchanger separated radioactive sodium in the primary system from nonradioactive sodium in the secondary system. Three secondary sodium loops transported reactor heat from the intermediate heat exchangers to the air-cooled tubes of the twelve dump heat exchangers. Instrumentation and control equipment provided monitoring and automatic control of the reactor and heat removal facilities; automatic reactor shutdown (SCRAM) if preset limits are exceeded; and computerized collection, handling, retrieval, and processing of operating and test data. Onsite utilities and services included emergency generation of electrical power, heating and ventilation, radiation monitoring, fire protection, and auxiliary cooling systems for plant equipment and components. The FFTF was the only U.S. liquid metal reactor built and maintained to American Society of Mechanical Engineers codes. Complementary standards were also developed for safety, testing, and quality assurance issues involved in liquid metal reactor technology. Facilities were included for receiving, conditioning, storing, and installing core components and test assemblies as well as examining and packaging for offsite shipment and radioactive waste disposal.

A picture of the FFTF plant and its location at the Hanford site in Washington State is shown in Figure B.1. Figure B.2 provides a diagram of the FFTF reactor plant and key parameters are listed in Table B.1. A cutaway of the reactor is shown in Figure B.3. Schematics of the primary and secondary coolant systems are shown in Figure B.4. Because it was designed as a flexible test reactor, the FFTF did not have steam generators but included dump heat exchangers. It was designed to provide a prototypic test bed with respect to temperature, neutron flux level, and gamma ray spectra for fast reactor fuels and materials testing. The FFTF was designed as the most extensively instrumented fast spectrum test reactor in the world, with proximity instrumentation of temperature and flow rate for each core component as well as contact instrumentation and gas and electrical connections for special test positions. Figure B.5 shows an FFTF instrumented test assembly.

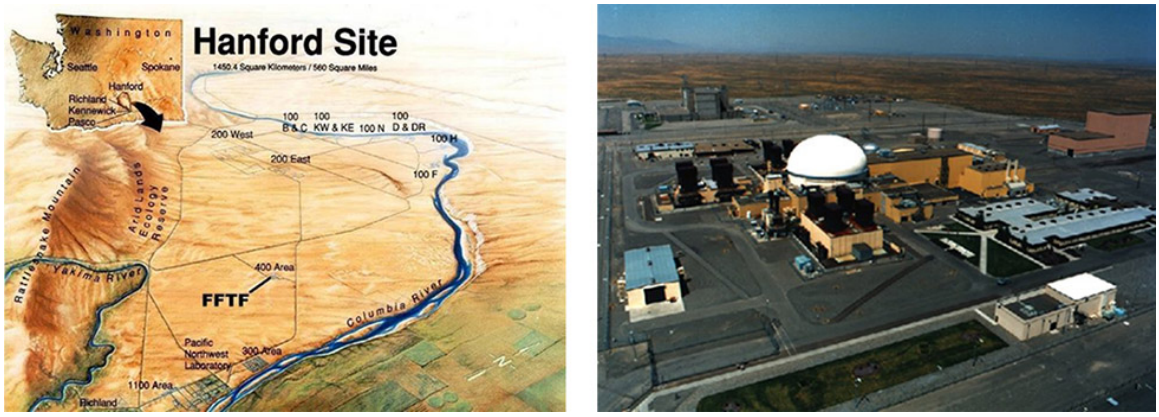

Figure B.1. FFTF at the Hanford Site

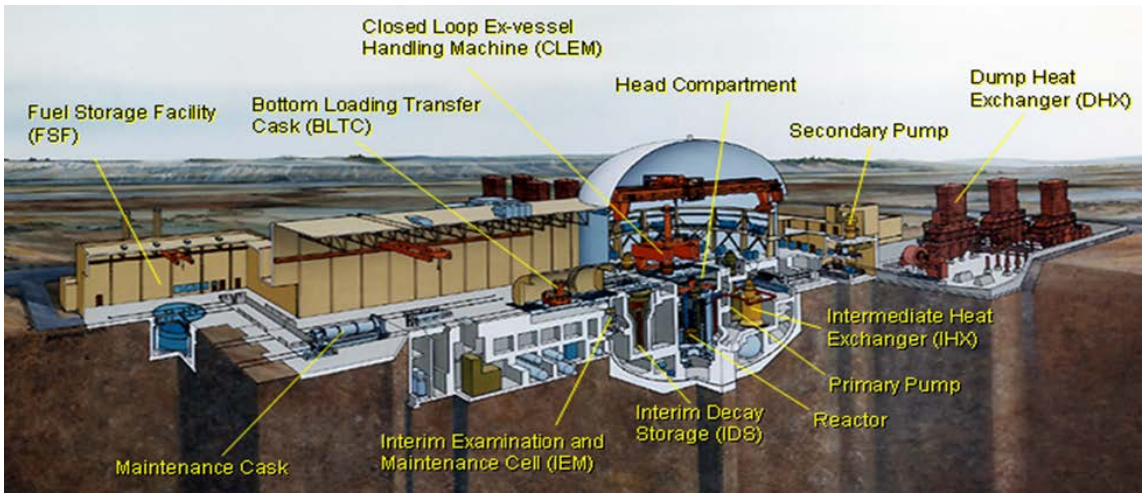

Figure B.2. FFTF Reactor Plant

Table B.1. FFTF Parameters

Parameter	Value
Thermal Power	400 MW
Coolant	Sodium
Coolant Inlet/Outlet Temperatures	360/526 C
Coolant Loops	3
Driver Fuel Material	$(Pu\text{-}U)O_2$
Enrichment Zones	2
Core Height	91.4 cm
Core Diameter	120 cm
In core Driver, Test Locations	82
Instrumented Through Head	8
Piping Length	64 km
Wiring Length	300 km
Instruments and Sensors	>20,000

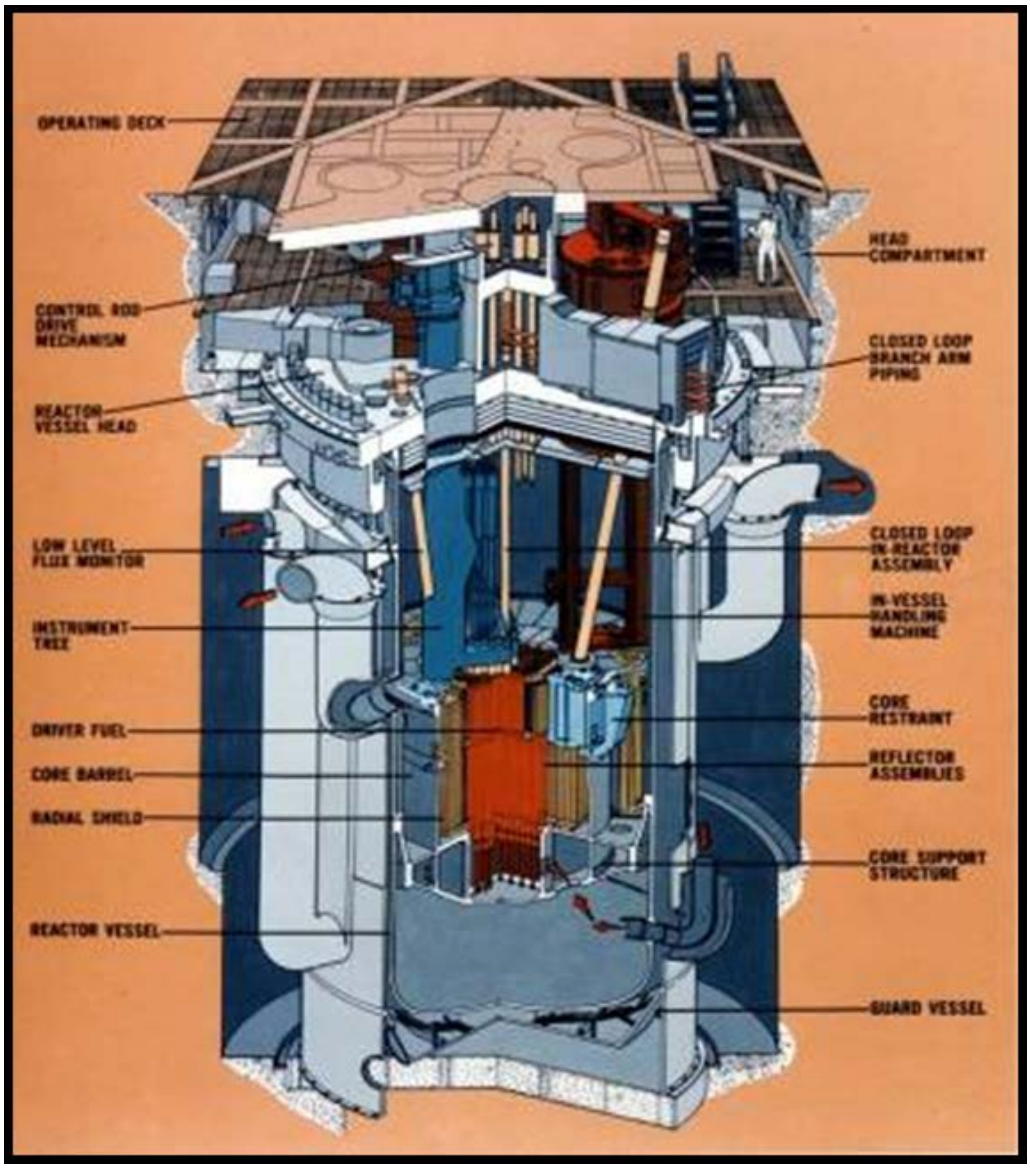

Figure B.3. FFTF Reactor

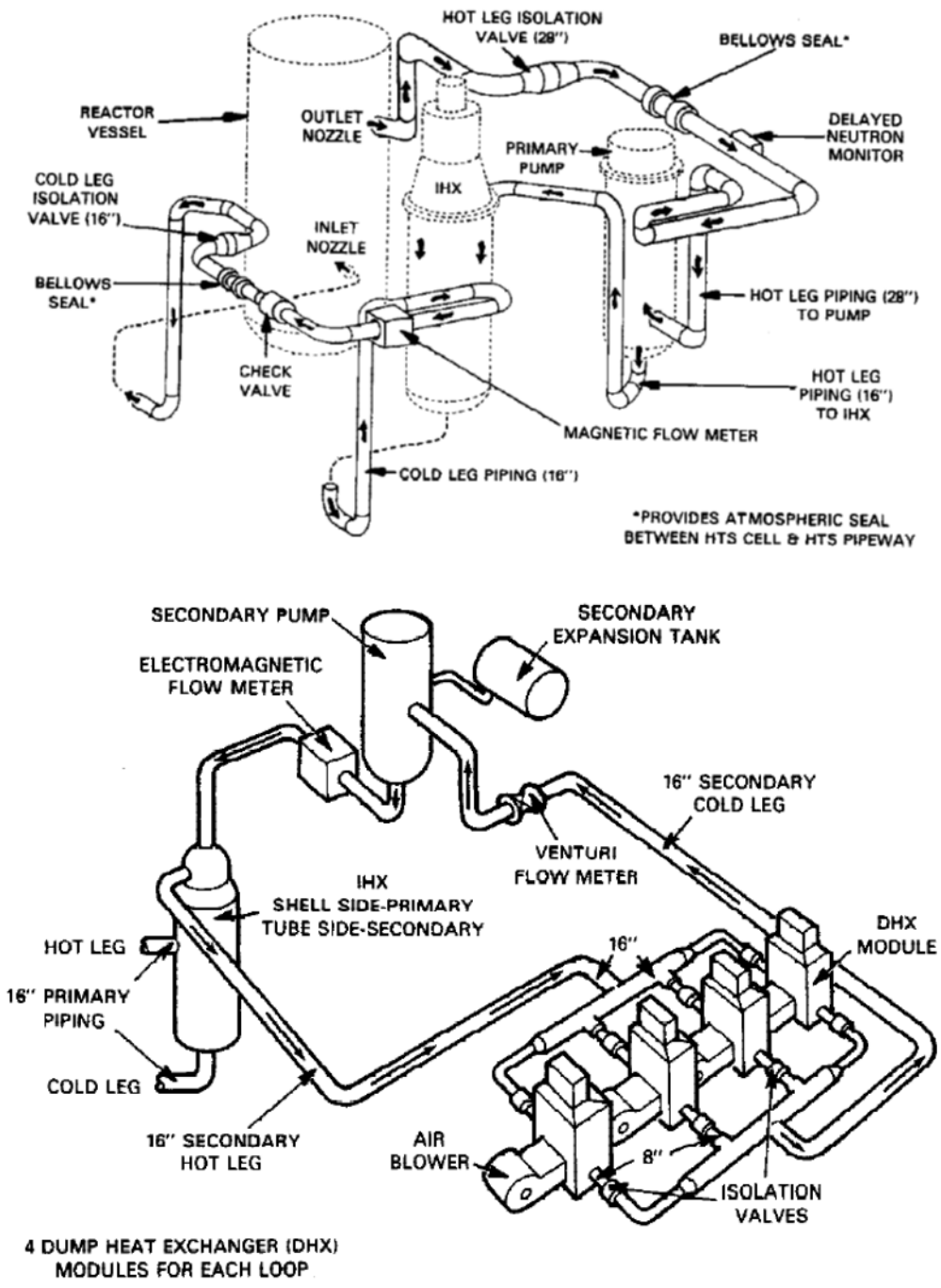

Figure B.4. FFTF Primary and Secondary Loop Schematics

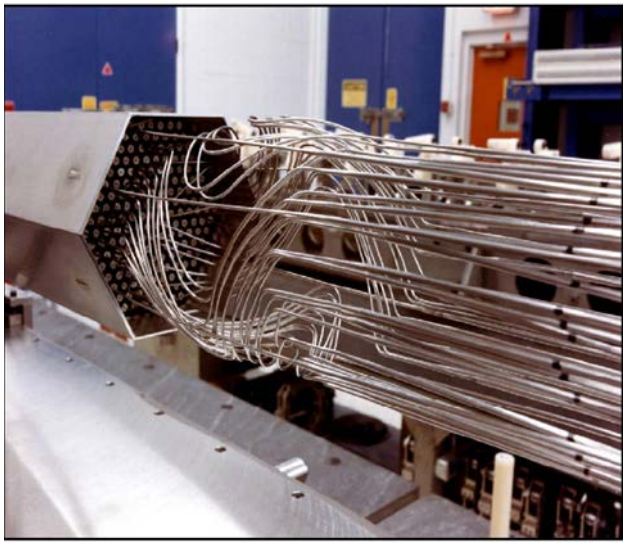

Figure B.5. Instrumented FFTF Test

Figure B.6 shows a timeline from the beginning of conceptual design to the first operating cycle. It is notable that during the 1960s and 1970s a substantial effort was expended in the development and testing of liquid metal reactor components. Figure B.7 shows the major activities during the twelve cycles of reactor operation. Safe, reliable, and economic operation of the FFTF was achieved through administrative controls, technical specifications, and operating procedures even with a demanding test schedule as a liquid metal irradiation test reactor. The high level of operating efficiency of FFTF provided vital data on the performance of liquid sodium as a safe and efficient heat transport medium and confirmed the reliability of many of its large-scale components.

FFTF was the most instrumented reactor in the world, with proximity instrumentation of temperature and flow rate for each core component as well as contact instrumentation and gas and electrical connections for special test positions. Detailed plant data acquired during operations and testing, such as assembly outlet temperatures and flow rates, coolant system temperatures and flow rates, and reactor vessel temperatures, were recorded on magnetic tapes by the plant data acquisition systems at frequencies up to once per second. During the years of operation, the FFTF plant data system systematically recorded over 1300 instrument variables. FFTF data measurement features include:

- Primary and secondary loop hot and cold leg temperatures and flow rates, neutron detectors, pump speed indicators
- Thermocouples with a response time of minutes were used to monitor assembly outlet temperatures for each core location
- Fast response thermocouples for measuring assembly outlet temperatures with a response time of seconds were used for two core locations during selected tests
- Two fuel tests included high response wire wrap thermocouples on fuel pins and were used during tests at startup
- The plant data system recorded >1300 variables at 0.1–60 second intervals.

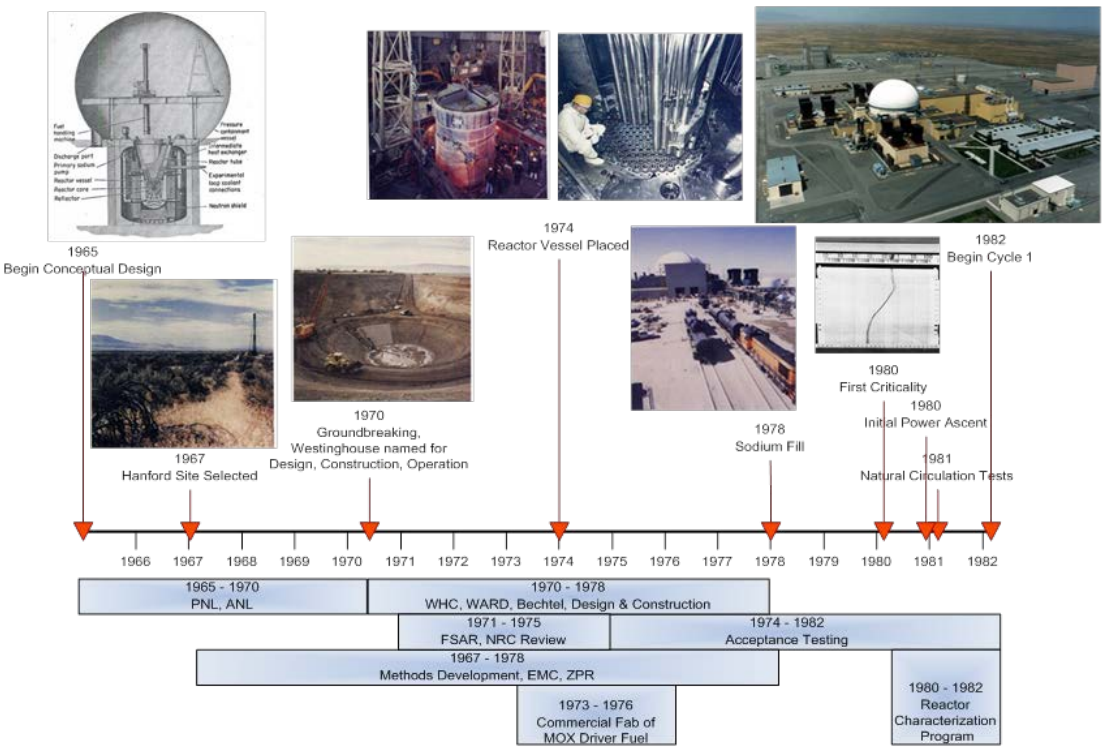

Figure B.6. FFTF History Prior to First Operating Cycle

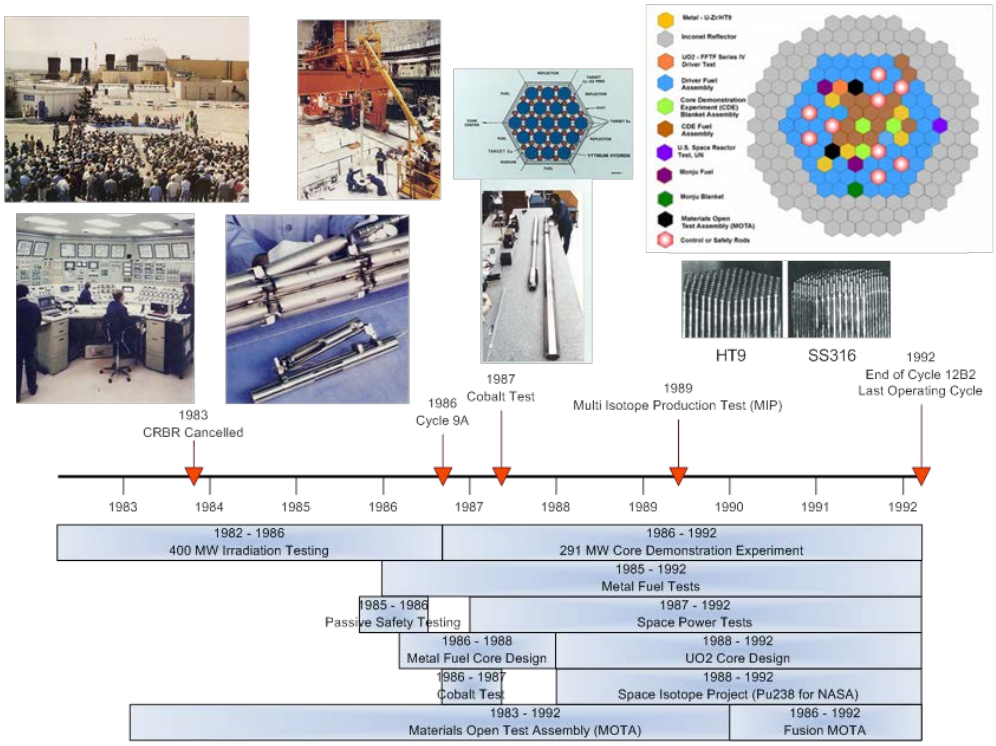

Figure B.7. FFTF Operating History

Documentation of the rigorous and successful design, construction, testing, and operational experience at FFTF was thorough and immense, with official records routinely archived. Efforts are currently directed at locating, extracting, and processing FFTF records of potential relevance to AdvSMR enhanced risk monitoring. Engineering knowledge from the design, construction, and operation of FFTF and other fast reactors represents a huge investment. Tapping this knowledge base is potentially worth billions of dollars, and at any valuation, will contribute to advanced fuel cycle designs. However, the FFTF information will not be useful if it is not accessible in a form that is useful and can be interpreted correctly. In order to ensure the FFTF information is useful, it is important to capture the tacit knowledge surrounding the documents and data. This tacit knowledge goes beyond what is printed on the pages of documents and includes the understanding of how the documents and data relate to one another historically, programmatically, and technically. Understanding of the context is important in navigating the collection of documents and data, recognizing the importance of specific data. Such tacit knowledge is not reproducible from electronic scans and knowledge must be captured from actual experts involved at the time.

B.2 FFTF Contribution to Enhanced Risk Monitoring

B.2.1 FFTF Data Potentially Relevant to AdvSMR Enhanced Risk Monitoring

FFTF data that is of potential use in developing enhanced risk monitoring is shown in Table B.2. The information has been separated into design, operations, and safety categories. Design information includes fabrication and procurement specifications, system design descriptions, and as-built drawings that can be used to pinpoint specific details on components such as valves, breakers, instrumentation, etc. The QA program specifies the controlled parameters for acceptance and testing of components. Operations data includes recorded sensor data, CREDO event reports, logs/records, and scheduled/unscheduled maintenance. The FFTF Job Control System (JCS) contains records of all work done at the plant, which would include maintenance and repair of components. Cycle operating and outage reports include descriptions of important activities and also list unusual occurrences during each cycle or outage. Safety data includes the safety analyses assumptions in the FSAR and from interactions with the NRC prior to operation. It also includes information that was gathered for the incomplete FFTF PRA effort.

B.2.2 CREDO

In 1977 the DOE established a CREDO at Oak Ridge National Laboratory (ORNL) to provide a centralized computer-based source of information on the reliability of components utilized in advanced liquid metal cooled reactors. The data were collected from operating reactors (EBR-II, FFTF, Joyo) and liquid metal loop test facilities and entered into the CREDO database on the ORNL mainframe until the program was terminated in 1992. During the ten years of FFTF operation, data forms were compiled into reports on FFTF events that were transmitted to CREDO. FFTF prepared and transmitted hundreds of CREDO Event Data Reporting Forms to ORNL over life of plant. Transmittal letters from FFTF were entered into records but attachments were typically not included. The CREDO database was only maintained at ORNL and was only available by access through ORNL. FFTF did not have a copy of the CREDO database. Currently no records of the CREDO database can be found.

Table B.2. Relevant FFTF Data

Mode	Type
Design	Fabrication specifications
	Procurement specifications
	Technical specifications
	Quality Assurance Program
	System Design Descriptions
	As-built drawings
Operations	Plant Sensor data
	CREDO data event reports
	Operational logs/records
	Maintenance/JCS database
Safety	FSAR approach
	NRC interactions
	Partial PRA/CAFTA input

Specific actions in progress at PNNL related to CREDO include:

- The few CREDO transmittals from FFTF that included CREDO forms are being collected.
- FFTF plant operations letterbooks are being searched for because they might contain the CREDO transmittals.
- FFTF plant Quality Assurance (QA) Vault records are being searched for CREDO files, because CREDO reporting was a function of the FFTF QA organization.
- A draft report, *Handbook of Component Reliability*, was located that contains various measures of component reliability and failure information for 13 component classifications from the CREDO database. This report includes the number of events by type, and overall failure rate, but no time frequency information. The 13 components were cold and vapor traps, electric heaters, filters/strainers, heat exchangers, logic gates, mechanical pumps, motors, non-nuclear sensors, pipes and fittings, pressure vessels and tanks, signal modifiers, support and shock devices, and valves.

Such processed CREDO component failure rate information are being examined for utilization in the simplified ERM framework AdvSMR PRA model described in Appendix A.

B.2.3 FFTF Event Descriptions Relevant to Component Reliability

During the ten years of FFTF operation, hundreds, maybe thousands, of events were recorded by FFTF operations and filed for every abnormal event that occurred. Efforts to locate a complete set of event fact sheets continue. Several records holding boxes containing FFTF operations files on occurrence reports with folders of histories of actions and resolutions related to the events have been located and are being examined for relevant component reliability information such as time frequency information for specific components and systems. The FFTF JCS contains records of all work done at the plant. Access to the FFTF JCS continues to be pursued. Once access is obtained, the intent is to search the JCS records for useful information.

During the late 1980s an effort was underway to prepare a PRA for FFTF. Part of that effort was to develop component failure rates by reviewing descriptions of events for that type of information. The FFTF PRA effort was terminated before it was complete, but resulted in over 200 event descriptions for significant events between 1980 and 1989 that were categorized into 18 internal event initiators, 6 internal leak locations, and external events for potential use in the preliminary FFTF PRA effort. This subset of event descriptions was retrieved and entered into a spreadsheet so that it could be searched for component reliability information. An example listing of a few of the events is shown in Table B.3. The FFTF PRA working files and system notebooks have also been located. These system notebooks and FFTF PRA information on specific components/systems are being used to guide the ERM PRA modeling. FFTF CAFTA working PRA input files were located on 5¼ inch floppy disks, but preliminary evaluation is that these files would be of little use in updating ERM methodology.

B.3 FFTF Summary

The ten years of successful operation of the FFTF provided a very useful framework that could potentially be used for determining the reliability of LMR technology components. Such component reliability data may be of increased importance to new designs after the events at Fukushima. Efforts to recover FFTF data useful for verifying ERM methodology have had limited success. FFTF CREDO database records have not been located. A subset of several hundred significant events collected and categorized during the preliminary FFTF PRA effort has been recovered. Efforts to extract component reliability information continue.

Table B.3. Example Listing of Preliminary FFTF PRA Events

Event Fact Sheet Number	Additional Documentation	Date	Nature of Problem	Location	Component	Cause	Explanation
80-003	HEDL 80-016	6/16/1980	Spurious Plant Protection System Trip	Control Room	Ratchet Puller Hoist	Maintenance Error	A ratchet puller hoist gave way, dropped detector, causing PPS shutdown signal
80-012		6/22/1980	Loss of Electrical Power	Control Room, RSS Panel C13DP	PPS System	Electrical Error	Ground located in PPS System during performance of SC-12-9
80-014		6/23/1980	Pump Failure	P-5 Pump Tower, cell	psi pressure controllers	Maintenance / Design Error	Supply reservoir went to 5 psi & cocked seal on secondary pump P-5 seal housing, causing oil to leak into lower seal leakage reservoir
80-015		6/24/1980	Inadvertent Sodium Leak	DHX - West	E-15 HV-43342	Electrical Error	Unexplained sodium flow from DHX E-15 drain valve HV-43342
80-018		6/25/1980	Cover Gas Pressure Transient	Control Room / Reactor Services Bldg	RAPS cold box	Operator / Design Error	RAPS cold box back pressurized due to reduced discharge path from CAPS maintenance
80-019		6/25/1980	Thermal Transient	DHX-East modules No. 2 and 4	pony motor gear box	Maintenance Error	Oil leakage from gear box sight glass led to high outlet temperature differential
80-023		7/4/1980	Inadvertent Valve Operation	Secondary Loop 1 drain piping	UV-43144	Electrical / Operator Error	Inadvertent opening of Secondary Loop 1 cold leg fill/drain valve resulting in transfer of Na to secondary drain header
80-024		7/5/1980	Pump Failure	Cell 556	P-52	Electrical Error	Overheating & improper heat up of P-52 Primary Sodium Sampling Pump
80-025		7/6/1980	Pump Failure	P-6 Pump Tower, Cell 461/435	Pump P-6 lower seal	Mechanical Error	P-6 lower seal cocked during routine shutdown of main motor; cause unknown
80-026		7/7/1980	Loss of Fire Protection System	C-1356, Zone 1	E-85 & E-86	Operator Error	Flow valves to detectors for E-85 & E-86 were isolated & hoses removed

Pacific Northwest
NATIONAL LABORATORY

U.S. DEPARTMENT OF
ENERGY

Proudly Operated by Battelle *Since 1965*

902 Battelle Boulevard
P.O. Box 999
Richland, WA 99352
1-888-375-PNNL (7665)
www.pnl.gov